Security Configuration Benchmark For

Apple OSX 10.6 Snow Leopard

Version 1.0.0
November 23rd, 2011

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**we**") agree and acknowledge that:

No network, system, device, hardware, software or component can be made fully secure;
We are using the Products and the Recommendations solely at our own risk;

We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights." Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules. CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

Overview

This document, *Security Configuration Benchmark for Apple OS X 10.6*, provides prescriptive guidance for establishing a secure configuration posture for Apple OSX 10.6. This guide was tested against Apple OSX 10.6. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Consensus Guidance

This benchmark was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in to the CIS benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Apple OSX 10.6.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Typographic Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Configuration Levels

This section defines the configuration levels that are associated with each benchmark recommendation. Configuration levels represent increasing levels of security assurance.

Level-I Benchmark settings/actions

Level-I Benchmark recommendations are intended to:
- be practical and prudent;
- provide a clear security benefit; and
- do not negatively inhibit the utility of the technology beyond acceptable means

Level-II Benchmark settings/actions

Level-II Benchmark recommendations exhibit one or more of the following characteristics:
- are intended for environments or use cases where security is paramount
- acts as defense in depth measure
- may negatively inhibit the utility or performance of the technology

Scoring Status

This section defines the scoring statuses used within this document. The scoring status indicates whether compliance with the given recommendation is discernable in an automated manner.

Scorable

The platform's compliance with the given recommendation can be determined via automated means.

Not Scorable

The platform's compliance with the given recommendation cannot be determined via automated means.

1 Recommendations

1.1 Installation Action Items

Security starts when the operating system is installed. There are a number of items to consider when a new system is set up for the first time, or when an existing system is repurposed.

1.1.1 Securely erase the Mac OS X partition before installation

Explanation	One never knows what is on a hard drive when one receives a computer, even new from Apple. Spyware or other malware may be present on a hard drive, so the safest course of action is to erase (reformat) the drive. Using the erase capability of Disk Utility (found on the Mac OS X Install DVD) will only erase the directory structure of disk and leave its contents intact. To make sure everything on the disk is erased, the Secure Erase feature of the Disk Utility must be used.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	This process can take a long time.
Remediation	1. Boot from the Mac OS X Install DVD. 2. Select a Language. 3. Select Disk Utility from the Utilities menu. 4. Select the disk to install Mac OS X on in the left panel. 5. Select the "Erase" tab. 6. Click on the Security Option button. 7. Choose "Zero out data," and then the "OK" button. 8. Click the "Erase" button.
Audit	None
Additional Info	None

1.1.2 Do not connect to the Internet when setting up a Mac

Explanation	The internet is where most of the bad stuff is located, so connecting to the internet can expose the Mac to attacks and malware. When setting up a Mac it is a good idea not to connect to the internet until the Mac is secure.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	May require extra hardware
Remediation	The primary reason to connect to the internet before a Mac is secure is to update the operating system. There are three options to provide additional safety when updating and securing a Mac before connecting it to the internet at large: 1. Install all the necessary updates from local media. 2. Connect the computer directly to a hardware firewall/router with no other computers connected to the firewall/router. Use Software Update to update the computer. 3. Update from a trusted Mac OS X Server's Software Update service on an isolated internal network.
Audit	None

Additional Info	None

1.1.3 Install Mac OS X using Mac OS Extended Journaled disk format

Explanation	This type of file system is the most compatible and supports all of the built-in security features of Mac OS X.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	None
Audit	None
Additional Info	None

1.1.4 Do not install any unnecessary packages

Explanation	Unneeded software unnecessarily increases the attack surface of the system.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	If the software is later needed, it will need to be installed and updated.
Remediation	In the "Easy Install on partition_name" step, click "Customize." Deselect any packages, languages, or print drivers that you do not plan on using. Do not install X11 unless the user has a need for it.
Audit	None
Additional Info	Use of disk imaging technology, such as Apple System Image Utility (included with Mac OS X Server) or other third party image utilities, is recommended wherever a standard image can be used. Deployment of standard images is beyond the scope of this document, but a list of some imaging technologies is listed in Appendix A.

1.1.5 Remove any unnecessary Applications or packages

Explanation	Unneeded software unnecessarily increases the attack surface of the system.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	If the software is no longer needed, it should be removed.
Remediation	Use the appropriate method recommended by the vendor to remove unneeded software. If there is no simple way to remove all component parts from the Operating System a clean install or re-image may be necessary
Audit	None
Additional Info	Use of disk imaging technology, such as Apple System Image Utility (included with Mac OS X Server) or other third party image utilities, is recommended wherever a standard image can be used. Deployment of standard images is beyond the scope of this document, but a list of some imaging technologies is listed in Appendix A.

1.1.6 Do not transfer confidential information in Setup Assistant

Explanation	The Setup Assistant will prompt the user for name, address, phone number, e-mail address, and other information. If you don't want personal information

	transferred to Apple, skip this step.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	In the Registration Information screen, press Command-Q to quit. Click the "Skip" button to bypass the registration process.
Audit	None
Additional Info	None

1.1.7 Create administrator accounts with difficult-to-guess names

Explanation	Simple names like "Administrator" or "Admin" are easy to guess, and provide an attacker some information needed to break into a system. Use a difficult-to-guess name for accounts with administration privileges to the Mac
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	When creating the first account in the Setup Assistant, use a difficult-to-guess name.
Audit	None
Additional Info	This applies to both the long name and short name, either of which may be used to log in to the computer through various login mechanisms. The short name is likely to have the widest exposure.

1.1.8 Create complex passwords for administrator accounts

Explanation	Passwords are the primary protection against unauthorized access. Accounts with administrative privileges are the most important to protect. Therefore, using a complex password for these accounts is very important.
Context	User
Level	1
Caveats	A complex password may be difficult to remember, so some users will write them down. If the password is written down, it should be kept is a safe place, preferably sealed in an envelope and locked up.
Remediation	Apple provides a Password Assistant in the dialogs used to set password. When setting a password, click on the key icon to the right of the New Password field to display the assistant. Make sure the password for the administrator account shows a quality of green. Make sure the quality meter is about halfway across or more. Alternatively, use a password that is at least 15 characters, and three of the following four items. Make sure the password does not contain a name or word found in the dictionary. Local passwords should not be reused on other devices for other purposes. Passwords and devices will be compromised, unique passwords reduce the risk. • Uppercase letter • Lowercase letter

	• Punctuation characters • Numbers
Audit	None
Additional Info	If you are color blind you may not be able to determine the quality of the password from the password assistant. However, numeric password quality information may be retrieved by hovering the cursor over the quality meter. The `pwpolicy` tool can be used to enforce password policies in Mac OS X directory services, but the policies do not apply to administrator-level users.

1.1.9 Do not enter a password-related hint

Explanation	A password hint will help you remember your password, but may also help an attacker to guess your password.
Context	User
Level	1
Scoring Status	Not Scorable
Caveats	The absence of a password hint may make remembering a password more difficult. Additionally, if using FileVault, not setting a hint may not allow a user to use a Master Password to reset a user account password.
Remediation	In the System Preferences: Accounts: Change Password dialog, enter the appropriate hint.
Audit	None
Additional Info	Organizations might consider entering an organizational help desk phone number or other text (such as a warning to the user). A help desk number is only appropriate for organizations with trained help desk personnel that are validating user identities for password resets.

1.1.10 Update system software using verified packages

Explanation	When manually downloading update packages from Apple (or other locations), always verify that what you downloaded is what you think it is. On the Apple download page there should be an SHA-1 Digest for the download. This long series of numbers and letters that is the result of a computer algorithm that is unique to the package download. Also, when looking at Apple's Web page to read the SHA-1 Digest, make sure you are visiting Apple's site using HTTPS.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	Verifying the SHA-1 digest requires the use of Terminal.
Remediation	See http://docs.info.apple.com/article.html?artnum=75510
Audit	None
Additional Info	Apple has a good explanation of how to use the SHA-1 Digest at http://docs.info.apple.com/article.html?artnum=75510

1.2 Hardware and Core Mac OS X Action Items

The easiest way to break into a Mac is with physical access to the computer. Restricting physical access is a very important step when protecting a computer.

1.2.1 Use an EFI password

Explanation	EFI (Intel) is the Mac equivalent of the BIOS on a PC. The Basic Input/Output System (BIOS) is a small piece of computer code embedded in the computer that lets the computer boot up. There are a few options that can be set in EFI, and should only be set by experienced administrators. One of the most commonly used options is a password. The firmware password will not prevent the computer from booting, but is required when booting from different media, such as an external drive, a CD or DVD disc, or a NetBoot volume, which can protect a computer from someone booting and quickly changing an account password with an install disk.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	Resetting the password is not overly difficult, but does require physical access and changes to the hardware. Also, the encryption used for firmware passwords is not strong; it is not overly difficult to retrieve the password, so using a common password is not recommended.
Remediation	Use the Firmware Password Utility to set a firmware password.
Audit	Open the Firmware Password Utility and verify the "Require password to change firmware settings" checkbox is checked.
Additional Info	When a firmware password is present, it must also be entered to: • boot into single user mode, which provides root access by default • boot into verbose mode • start up in Target Disk Mode to access the internal hard disk (and on some models, the optical drive) from another computer. A firmware password may disable FireWire DMA access, but this appears to be undocumented. http://docs.info.apple.com/article.html?artnum=106482 https://support.apple.com/kb/ht1352

1.2.2 Create an access warning for the login window

Explanation	Displaying an access warning that informs the user that the system is reserved for authorized use only, and that the use of the system may be monitored, may reduce a casual attacker's tendency to target the system. Access warnings may also aid in the prosecution of an attacker by evincing the attacker's knowledge of the system's private status, acceptable use policy, and authorization requirements.

Context	System
Level	1
Scoring Status	Scorable
Caveats	Requires use of Terminal to set the banner text.

Remediation	To add text with elevated privileges:
	
	`sudo defaults write /Library/Preferences/com.apple.loginwindow \`
	`LoginwindowText "your text here"`
	
	To remove the text with elevated privileges:
	
	`sudo defaults delete /Library/Preferences/com.apple.loginwindow`
	`LoginwindowText`

Audit	Run the following command to see the login window text:
	`defaults read /Library/Preferences/com.apple.loginwindow.plist`
	`LoginwindowText`

Additional Info	None

1.2.3 Create an access warning for the command line

Explanation	There are two common ways to login to a Mac using the command line, bypassing the GUI login window: FTP and SSH. Displaying an access warning that informs the user that the system is reserved for authorized use only, and that the use of the system may be monitored, may reduce a casual attacker's tendency to target the system. Access warnings may also aid in the prosecution of an attacker by evincing the attacker's knowledge of the system's private status, acceptable use policy, and authorization requirements.
Context	System
Level	2
Scoring Status	Scorable
Caveats	The banner will be displayed before the user logs in. This may interfere with scripted logins.
Remediation	Create a text file with the login text. This is commonly done in `/etc/motd` for SSH and `/etc/ftpwelcome` for FTP. For SSH, edit `/etc/sshd_config` (using sudo) and add the line: `Banner /etc/banner` Where `/etc/banner` is the path to your login banner text file.
Audit	Run the following commands to determine if the banner text is set: `cat /etc/sshd_config	grep Banner` If there is a valid entry for Banner, cat the path show and view the results.
Additional Info	see `man sshd_config`

1.2.4 Turn on file extensions

Explanation	By making the file extension visible, you can determine the type of file it is and

	the application it is associated with. It is fairly simple for malicious code or unapproved software to appear as if it is something other than what it is. File Types should be visible
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	Users may prefer not seeing extensions in their environment
Remediation	1. Open Finder. 2. From the Finder menu, select Preferences. 3. Click Advanced and select the "Show all filename extensions" checkbox.
Audit	
Additional Info	None

1.2.5 Disable Bluetooth

Explanation	Bluetooth is a very useful technology, but it also can expose a Mac to certain risks, if Bluetooth is not allowed in your environment use these settings. Bluetooth can be disabled via software or hardware. Temporary disablement via System Preferences will be discussed in Section 2.4.10.4. To completely secure Bluetooth, the Bluetooth hardware should be removed from the Mac. Alternatively, and somewhat less secure: • remove the Bluetooth extensions (drivers) from the operating system • disable the Bluetooth process using `launchd` • use MCX settings to disable Bluetooth
Context	System
Level	2
Scoring Status	Scorable
Caveats	Removing the Bluetooth hardware may void the Mac's warranty and should only be done by an authorized Apple technician. Software disablement will not completely secure the Bluetooth as the software can be reinstalled.

Remediation	1. Have an authorized Apple technician remove the Bluetooth hardware from the Mac.
	
	2. Remove the following files from `/System/Library/Extensions` and reboot the Mac:
	
	`IOBluetoothFamily.kext`
	`IOBluetoothHIDDriver.kext`
	
	3. Run `sudo launctl unload -w /System/Library/LaunchDaemons/com.apple.blued.plist`
	
	4. Use a Mac OS X Server or Apple's free WorkGroup Manager (part of the Server Administration Tools) to disable Bluetooth.

Audit	Run the following command to determine if Bluetooth is present. Note: This command cannot distinguish between software or hardware disabled Bluetooth.

| | ```
system_profiler SPBluetoothDataType
``` |
| Additional Info | None |

1.2.6 Disable the iSight camera

Explanation	The iSight camera built-in to many Macs can allow a remote attacker to watch and view potentially sensitive information. External iSight cameras (and other brands too) should be disconnected when not in use. Internal iSight cameras should be disconnected if required by the organization. If video conferencing is not required in your organization the camera should be covered and the software should be disabled. Vulnerabilities have been identified with software that have taken control of built-in cameras and if there is not a business need the future vulnerabilities have already been mitigated if disabled.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	Disabling the internal iSight camera may void the Mac's warranty and should only be done by an authorized Apple technician.
Remediation	Have an authorized Apple technician disconnect the internal iSight camera. Alternatively, but less secure, place opaque tape or label over the camera lens. Consider removing or altering the following file to disable iSight capabilities: ```/System/Library/Extensions/Apple_iSight.kext```
Audit	Run the following command to determine if an iSight is present. ```system_profiler SPUSBDataType	grep iSight```
Additional Info	None

1.2.7 Reduce the sudo timeout period

Explanation	The ```sudo``` command is used by a user to elevate privileges. By default, privileges will remain escalated for 5 minutes after the ```sudo``` command is completed. During this time, the ```sudo``` command can be executed again without authentication. This window of opportunity should be eliminated.
Context	System
Level	2
Scoring Status	Scorable
Caveats	None

Remediation	Execute the following command in Terminal. This command required knowledge of the "vi" editor.
	
	```sudo visudo```
	
	In the "```# Defaults specification```" section, add the line:
	
	```Defaults timestamp_timeout=0```

Audit	Run the following command:

```
sudo cat /etc/sudoers | grep timestamp
```

and make sure the result is:

```
Defaults timestamp_timeout=0
```

Additional Info	None

1.2.8 Remove unneeded QuickTime components

Explanation	QuickTime provides a modular architecture that allows for components to increase the number of media types QuickTime understands. These add-in components can be used in whatever context QuickTime runs. While these components can be used in local applications, the QuickTime plug-in allows browsers (including any that are based on WebKit) to play embedded content in the Web pages. If a particular QuickTime component, such as a codec, is not needed then consider removing it. This reduces the kind and number of media that could be used as vectors for attack in a web environment.
Context	System and User
Level	2
Scoring Status	Not Scorable
Caveats	A component may be required at a later date to play content. The component may be reinstalled through various software updates or software installs. Removal of a component that is a default part of the QuickTime installation may require the reinstallation of QuickTime or the entire operating system, particularly if that software was installed within the system domain (or "/System"). This also prevents the playback of media types supported by a QuickTime component opened locally in applications.
Remediation	QuickTime components are stored in `/Library/QuickTime` and `~/Library/QuickTime`. Other components are stored in the system domain at `/System/Library/QuickTime`, where removal is not recommended. Additional Internet plug-ins for browsers, which may or may not have a relationship with QuickTime, may be found in the local domain at `/Library/Internet Plug-ins` as well as in the user domain at `~/Library/Internet Plug-ins`. Any unneeded Internet plug-ins may be removed.
Audit	None
Additional Info	Opening media types in local applications could be an attack vector for documents attached to e-mail or stored/transferred in other ways. Viewing the same media in a Web browser may be considered riskier since the data could be coming from an untrusted source and will likely be interpreted immediately by the browser. Some optional QuickTime components, such as additional codecs, can be obtained through the QuickTime System Preferences pane. It links to this Web page:

	http://www.apple.com/quicktime/resources/components.html

1.2.9 Disable Core Dumps

Explanation	When an application encounters a runtime error the operating system has the opportunity to dump the application's state, including memory contents, to disk. This operation is called a core dump. It is possible for a core dump to contain sensitive information, including passwords. Therefore it is recommended that core dumps be disabled in high security scenarios.
Context	System and User
Level	2
Scoring Status	Scorable
Caveats	None
Remediation	Run the following command: `launchctl limit core 0`
Audit	Run the following command: `launchctl limit core`
Additional Info	For more information, execute "man core"

1.3 Account Configuration Action Items

Account management is critical to computer security. Accounts are comprised of account information and, for some account types, a home directory for storage of settings and files.

The account information in Snow Leopard is stored in the new DSLocal store, which replaces the legacy NetInfo service used in previous versions of Mac OS X. The DSLocal store is a filesystem hierarchy of individual property list (plist) files, rather than a database (as in NetInfo) or a set of flat files (as might be seen in other Unix systems).

Mac OS X provides for a number of different types of accounts, each with different levels of default privileges. Each account type needs to be secured.

- An administrator account has full privileges, largely because of its membership in the local `admin` group. Members of this group are granted access to portions of the file system outside of its own home folder, especially in the system domain (such as `/Library`). By default, members of "admin" also have `sudo` rights. An administrator account is sometimes referred to as a privileged account.
- A standard account has a medium level of privileges, generally providing access only to only its own settings, folders, and files.
- A managed account is equivalent to a standard account with the addition of Parental Controls or Managed Client (MCX) settings applied to it. While a managed account can log in and store data or settings in its home directory, further restrictions can be enforced on it. These restrictions are defined in Accounts System Preferences for Parental Controls.
- A sharing only account is roughly equivalent to a standard account. Its shell is set to

`/usr/bin/false` and it does not have login access. It has no home directory (which is set to `/dev/null`). It can have access to some other portions of the file system, such as temporary space, as a member of the `staff` group. A sharing only account is meant solely for access to the local system's sharing services, as seen in the Sharing System Preferences, as well as any other sharing features enabled by applications that use the Identity Services system.

- The guest account has the least privileges. It is meant for temporary access to the system. The guest account is similar to a standard account whose settings are purged between logins. It requires no password.

More information on the different types of accounts is available in Apple's Identity Services documentation at:

http://developer.apple.com/documentation/Networking/Conceptual/IdentityServices_ProgGuide/architecture/chapter_2_section_4.html#/apple_ref/doc/uid/TP40004490-CH3-DontLinkElementID_8

Each user should have an account to ensure that their settings and documents are kept separate. This can provide compartmentalization, so that compromise of one does not necessarily lead to another. Even with kids on the family computer, each user should have their own account, which can make it easier to apply individual controls (such as enforced time limits or applications that can be launched) to them.

Each user should try to run with the least privileges necessary for whatever they are doing on the computer. This also provides compartmentalization, since users with lower privileges have less access system-wide to settings and the file system.

Never have shared accounts, and take special note of how the guest account is similar to one.

Managed accounts are subject to Parental Controls or MCX settings, which both use the same underlying account control mechanisms in the operating system. The settings can be applied locally or remotely. Parental Controls can be shared between Snow Leopard-based computers (see the Parental Controls System Preferences pane). MCX settings can be applied from a directory service with Apple's schema additions.

It is important for some environments to note that Snow Leopard enables a local Kerberos Key Distribution Center (KDC) for the accounts specific to each computer. This is used with the new Identity Services system in Snow Leopard to support sharing. For more on Identity Services, identities, and their Access Control Lists (ACLs) see:

http://developer.apple.com/documentation/Networking/Conceptual/IdentityServices_ProgGuide/Introduction/chapter_1_section_1.html

1.3.1 Create an administrator account and a standard account for each administrator

Explanation	An administrator account should rarely be used. In most cases when administrative privileges are needed, the Mac will prompt the user for a user name and password. There are some operations where logging in as an administrator is necessary, but these are rare.
	The reason to not regularly use an administrator account for daily operations is security. Many operations that affect security can be accomplished without a

	password when an administrator is logged in. When logged in as a standard user, very few, if any, of the operations that affect the entire computer are possible without authentication to obtain elevated privileges.
Context	User
Level	1
Scoring Status	Not Scorable
Caveats	Administrators have unrestricted write/delete access to various directories, including `/Applications` and `/Library`. Administrators, by default, can escalate themselves to have access to any directory on the computer. Care should be given when granting a user administrative access.
Remediation	Do not log in with an administrator account unless necessary.
Audit	Open System Preferences: Accounts and verify there is a regular user account for each administrator.
Additional Info	If administrator rights need to be controlled, consider granting specific `sudo` rights to individual users as needed. In larger environments, you may wish to grant administrator rights only to directory service-based groups.

1.3.2   Create a standard or managed account for each non-administrator

Explanation	A non-administrator should not need administrator privileges on the Mac, so create a standard (or managed, if using Mac OS X Server or Parental Controls) account for these users.
Context	User
Level	1
Scoring Status	Not Scorable
Caveats	Standard users have reduced rights which may affect their ability to alter things on the computer. Standard users cannot install software in the `/Applications` folder and cannot change various System Preferences, including creation and modification of network settings or the computer's time zone. Standard users can still make some changes, such as switching between administrator-defined network locations.
Remediation	Do not give the "Allow user to administer this computer" right to standard users in System Preferences: Accounts.
Audit	None
Additional Info	If you need to grant specific rights to non-administrator users, such as the ability to change time zones, consult the Apple support knowledgebase. Some of these rights can be changed in the authorization rights database, `/etc/authorization`, and Apple does provide articles for common ones.

1.3.3 Set appropriate parental controls for managed accounts

Explanation	Many aspects and features of the Mac can be restricted on a user-by-user basis, including computer usage time limits. Although this feature is called Parental Controls, these restrictions may be appropriate for corporate, government, or educational use.
Context	User
Level	1
Scoring Status	Not Scorable

Caveats	None
Remediation	In the System Preferences: Accounts or in WorkGroup manager, activate Parental Controls and set the appropriate controls for each standard user.
Audit	None
Additional Info	Parental Controls typically apply locally, although in Snow Leopard they can be shared between computers. For wider deployments, consider the use of the Apple MCX schema in your directory service; it is available in Mac OS X Server by default.

1.3.4 Restrict sudo users to being able to access only required commands

Explanation	The `sudo` command allows a user to execute a command in Terminal as another user, typically the "root" user. By default, standard users cannot use the `sudo` command and administrator users can use all commands via `sudo`. Specific commands can be restricted to specific users or groups as needed.
Context	System and User
Level	2
Scoring Status	Scorable
Caveats	Restriction of the `sudo` command can be complicated and should only be implemented by an experienced system administrator.
Remediation	Always use the `visudo` command to edit the `/etc/sudoers` file. Read the `man sudo` page for more information.
Audit	Run the following command and verify the correct groups and user and the correct authorities. `sudo cat /etc/sudoers`

Additional Info	`man visudo`
	`man sudo`
	`man sudoers`

1.3.5 Securely configure LDAPv3 access

Explanation	When configuring LDAPv3, you should not add DHCP-supplied LDAP servers to automatic search policies. Whenever possible, use authenticated and encrypted LDAP connections.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	When using authenticated and/or encrypted connections, the LDAP server must support these options.
Remediation	Proper and secure configuration of LDAP is beyond the scope of this document. Make sure to have an experienced LDAP administrator configure and secure the connection.
Audit	None
Additional Info	None

1.3.6 Securely configure Active Directory access

Explanation	When configuring Active Directory on the Mac client, verify that all the settings are correct. Specifically, make sure that the: • UID and GID mapping (if used) are appropriate

	• The list of groups of OS X administrators that can administer the Mac (if used) is configured as intended.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	None
Remediation	Proper and secure configuration of AD is beyond the scope of this document. Make sure to have an experienced AD administrator configure and secure the connection.
Audit	None
Additional Info	None

1.3.7   Use Password Assistant to help generate complex passwords

Explanation	Passwords are the primary protection against unwanted access.
Context	User
Level	1
Scoring Status	Not Scorable
Caveats	A complex password may be difficult to remember, so some users will write them down. If the password is written down, it should be kept is a safe place, preferably sealed in an envelope and locked up.
Remediation	Apple provides a Password Assistant in the dialogs used to set password. When setting a password, click on the key icon to the right of the New Password field to display the assistant. Make sure the password for the administrator account shows a quality of green. If you are color blind you may not be able to determine the quality of the password from the Password Assistant. Make sure the quality meter is about halfway across or more, or hover over the meter to see its calculated entropy value in a tooltip. For the entropy value, higher is better.
Audit	None
Additional Info	None

1.3.8 Set a strong password policy

Explanation	Mac OS X Server allows the use of centrally managed password policies. If possible, use this feature to set a strong policy for passwords.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	Mac OS X Server and a managed Mac environment are required for centralized management.
Remediation	Determining a strong policy and making the appropriate settings in Mac OS X Server is beyond the scope of this document.
Audit	None
Additional Info	Apple provides the `pwpolicy` command which can set some policies locally, without a Mac OS X Server. See `man pwpolicy` for more information. Note that many of the options are not available without Mac OS X Server (and are not documented as such). Also note that use of the `pwpolicy` command is not enforced for administrators or for users when using the CLI `passwd` command.

1.3.9 Automatically lock the login keychain after 15 minutes of inactivity and when sleeping

Explanation	The keychain is a secure database store for passwords and certificates. A keychain is created for each user account on Mac OS X, and the system software itself uses keychains for secure storage. As of this writing, items secured in a keychain are encrypted with 3DES, while the directory or metadata information is available in clear text. For example, when Safari asks if you want to save a password and you answer yes, the password is stored in the default keychain. Many applications are keychain aware, others like Firefox and Thunderbird have their own dedicated password managers by default All keychain aware applications store their passwords in a keychain (Login Keychain by default.) In order to protect those credentials the keychain should lock automatically after 15 minutes or an organizationally defined value
Context	User
Level	1
Scoring Status	Scorable
Caveats	If the timeout is set too low on heavily used items the user will be annoyed and may use workarounds.
Remediation	1. In `Keychain Access`, Select the keychain 2. Choose `Edit > Change Settings for keychain <`*`keychain_name`*`>`, and authenticate, if requested. 3. Change the `Lock after # minutes of inactivity` setting for the Login Keychain to `15 minutes` or based on the access frequency of the security credentials included in the keychain for other keychains.
Audit	None
Additional Info	None

1.3.10 Secure the login keychain

Explanation	By default, the login keychain for an account, especially a local account, has the same password as the account's logon password. If the logon password is compromised, the login keychain would also be compromised. It is possible to change the password on the login keychain to something different than the logon password, and doing so would keep that keychain locked until it is needed after login.
Context	User
Level	2
Scoring Status	Not Scorable
Caveats	Having two different passwords can be an inconvenience. Logging in to an account would no longer unlock the login keychain by default. In environments using Directory authentication with regular or frequent mandated password changes there are both positive and negative repercussions in having a different password for the login keychain, particularly with FileVault use.
Remediation	Open `/Applications/Utilities/Keychain Access` Select login in the left panel

	Select Edit:Change Password for Keychain and change the password
Audit	None
Additional Info	None

1.3.11 Secure individual keychain items

Explanation	Each keychain entry can have different access controls. It's possible to set the keychain item to require a keychain password every time an item is accessed, even if the keychain is unlocked. This level of security could be useful for bank passwords or other passwords that need extra security.
Context	User
Level	2
Scoring Status	Not Scorable
Caveats	Having to enter the keychain password for each access could be inconvenient.
Remediation	In Keychain Access search for the entry to protect Open the Entry and click on the Access Control tab Make sure the Ask for Keychain password checkbox is checked
Audit	None
Additional Info	None

1.3.12 Create specialized keychains for different purposes

Explanation	A user can have more than one keychain. If the user can logically split password and other entries into different keychains with different passwords, a compromise of one password will have limited effect.
Context	User
Level	2
Scoring Status	Not Scorable
Caveats	Using multiple keychains can be inconvenient. It is also not necessarily possible for all kinds of data, such as Safari auto-fill information, to be stored in secondary keychains. Not all keychain-aware applications may provide an interface to choose secondary keychains.
Remediation	Use Keychain Access to create multiple keychains. Store entries in the appropriate keychain when possible.
Audit	None
Additional Info	One useful separation of keychains might be in a business environment. Personal information might be stored in one keychain and business information in a different keychain.

1.3.13 Use a portable drive to store keychains

Explanation	Keychains are just files on the computer, and thus do not need to be stored on the computer. Storing a keychain file on a portable drive (such as a USB flash drive) could help protect the data in the event the computer were stolen or compromised.
Context	User
Level	2
Scoring Status	Not Scorable
Caveats	Using keychains stored on portable drives can be inconvenient. The portable drive needs to be protected and backed up. The potential for the portable drive being lost or stolen must be weighed against the security benefit.

Remediation	Copy the files from `~/Library/Keychains/` to a portable drive then securely delete the files on the computer.
Audit	None
Additional Info	None

1.3.14 Do not enable the "root" account

Explanation	The `root` account is a superuser account that has access privileges to perform any actions and read/write to any file on the computer. In the UNIX/Linux world, the system administrator commonly uses the root account to perform administrative functions. On a Mac, root should not be enabled. In any circumstance an administrator can escalate privileges using the `sudo` command (use `-s` or `-i` to get a root shell). By default the root account is not enabled on a Mac OS X client computer. It is enabled on Mac OS X Server.
Context	System
Level	1
Scoring Status	Scorable
Caveats	UNIX/Linux system administrators need to learn to use `sudo -s` instead of `su -`. Also, `sudo` on the Mac is not Kerberized, but can be with a free third party PAM module.
Remediation	Nothing specific; just don't enable root using the Directory Access program (in `/Applications/Utilities/`), with the CLI `passwd` command via `sudo`, or with the Reset Password utility on the installer DVD.

Audit	Open `/Applications/Utilities/Directory Utility` program and verify `root` is disabled.
	
	Alternatively, run the following command:
	
	`dscl . -read /Users/root AuthenticationAuthority`
	
	The result should be:
	
	`No such key: AuthenticationAuthority`

Additional Info	The `root` password, like those of other local user accounts, can still be reset when using the Password Reset Utility on the Mac OS X Install DVD. The `AuthenticationAuthority` attribute could also contain `;DisabledUser;` which would prevent logins by the account.

1.4 Securing System Software Action Items

Every system preference with security-related configuration settings has its own action item checklist.

1.4.1 MobileMe Settings

1.4.1.1   Do not enable or use MobileMe

Explanation	MobileMe was a service offered by Apple, Inc. that allows seamless integration between many Mac applications and Apple services. The service is deprecated and will be ended on June 30th, 2012 in favor of iCloud services available with IOS5 and with 10.7 (as of 10.7.2)
Context	User
Level	1
Scoring Status	Scorable
Caveats	None
Remediation	Do not enter a user name and password and connect to MobileMe

Audit	Open System Preferences: MobileMe for user and make sure the user name and password field are blank.
	
	Alternatively, run the following command for each user account:
	
	`defaults read ~/Library/Preferences/.GlobalPreferences iToolsMember`
	
	And ensure the results are blank or returns:
	
	`The domain/default pair of (.GlobalPreferences, iToolsMember) does not exist`

Additional Info	None

1.4.2   Accounts Preferences Action Items

Proper account management is critical to computer security. Many options and settings in the Account System Preference Pane can be used to increase the security of the Mac.

1.4.2.1   Change initial password for the system administrator account

Explanation	If you did not set the initial password to the Mac, the password should be changed for all accounts, including the administrator account, as soon as possible. If the initial admin account is not needed, the account should be deleted.
Context	User
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	In System Preferences: Accounts, select the user, then change the password or delete the account if not needed.
Audit	None
Additional Info	At least one admin account is required, although it does not necessarily need to be enabled or have a known password at any given time. The admin account could be disabled to prevent logins. Or, its password could be set to a strong, highly complicated password that is forgotten and not used. In such cases, you would need to re-enable the account or change its password before use. It should also be noted that an attacker who has the ability to remove the `/var/db/.AppleSetupDone` file can restart the computer and create a new administrator account from the Mac OS X Setup Assistant. The `.AppleSetupDone`

	file determines whether the system runs the Setup Assistant or not.

1.4.2.2 *Disable automatic login*

Explanation	Having a computer automatically log in bypasses a major security feature (the login) and can allow a casual user access to sensitive data in that user's home directory and keychain.
Context	System
Level	1
Scoring Status	Scorable
Caveats	None
| Remediation | In System Preferences: Accounts, Login Options, disable Automatic Login.<br><br>Note: Automatic login can also be disabled in System Preferences: Security.<br><br>Alternatively, run the following command<br><br>```
sudo defaults write /Library/Preferences/.GlobalPreferences \
com.apple.userspref.DisableAutoLogin -bool yes
``` |
| Audit | Open System Preferences: Accounts, Login Options, and verify Automatic Login is disabled.<br><br>Alternatively, run the following command:<br><br>```
defaults read /Library/Preferences/.GlobalPreferences \
com.apple.userspref.DisableAutoLogin
```<br><br>Make sure the value returned is 1. |
| Additional Info | None |

1.4.2.3 *Display login window as name and password*

Explanation	Displaying the names of the accounts on the computer may make breaking in easier. Force the user to enter a login name and password to log in.
Context	System
Level	1
Scoring Status	Scorable
Caveats	Users will need to remember their login name.
| Remediation | In System Preferences: Accounts, Login Options, select Name and Password<br><br>Alternatively, run the following command<br><br>```
sudo defaults write /Library/Preferences/com.apple.loginwindow \
SHOWFULLNAME -bool yes
``` |
| Audit | Open System Preferences: Accounts, Login Options, and verify Name and Password is selected.<br><br>Alternatively, run the following command:<br><br>```
defaults read /Library/Preferences/com.apple.loginwindow SHOWFULLNAME
``` |

	Make sure the value returned is 1.
Additional Info	None

1.4.2.4 Disable "Show password hints"

Explanation	Password hints can give an attacker a hint as well, so the option to display hints should be turned off. If your organization has a policy to enter a help desk number in the password hints areas, do not turn off the option.
Context	System
Level	1
Scoring Status	Scorable
Caveats	Might make remembering a password more difficult. If using FileVault, not setting a hint may not allow a user to use a Master Password to reset a user account password.
Remediation	In System Preferences: Accounts, Login Options, make sure the "Show password hints" checkbox is off. Alternatively, run the following command ```sudo defaults write /Library/Preferences/com.apple.loginwindow \ RetriesUntilHint -int 0```
Audit	Open System Preferences: Accounts, Login Options, and verify "Show password hints" checkbox is off. Alternatively, run the following command: ```defaults read /Library/Preferences/com.apple.loginwindow RetriesUntilHint``` Make sure the value returned is 0.
Additional Info	None

1.4.2.5 Configure "Allow network users to login to this computer"

Explanation	This option is only available is the Mac is configured to authenticate through a Directory Service (like Active Directory or Open Directory). The Options button will allow the computer to restrict which network user can log on to the Mac; the default is to allow all network users to log in. If there is no business need for all users to log in to the computer only those users that need to should be enabled
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	None
Remediation	In System Preferences: Accounts, Login Options, turn on "Allow network users to login to this computer," then click the Options button to configure logon access as needed.
Audit	None
Additional Info	None

1.4.2.6 Disable "Enable fast user switching"

Explanation	Fast user switching allows a person to quickly log in to the computer with a different account. While only a minimal security risk, when a second user is logged in, that user might be able to see what processes the first user is using, or possibly gain other information about the first user.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	Security benefit of not allowing fast user switch is of limited value.
Remediation	In System Preferences: Accounts, Login Options, make sure the "Enable fast user switching" checkbox is off.
Audit	In System Preferences: Accounts, Login Options, make sure the "Enable fast user switching" checkbox is off.
Additional Info	Mac OS X is a multi-user operating system, and there are other similar methods that might provide the same kind of risk. The Remote Login service that can be turned on in the Sharing System Preferences pane is another.

1.4.2.7 Disable "Allow guest to log into this computer"

Explanation	The Guest account allows a guest to log in to a Mac and use all of its services. When the guest logs out, the Mac clears most of whatever the guest did on the Mac. This allows one person to let another borrow the computer for a short period, and still protect information in other accounts on the Mac. The usage of a Guest account may give the Mac owner a false sense of security. If the guest has physical access to the Mac and the owner is not present, the guest could gain full access to the Mac. That said, use of the Guest account allows for quick and moderately safe computer sharing.
Context	System
Level	1
Scoring Status	Scorable
Caveats	None

Remediation	In System Preferences: Account, click on the Guest user.
	Make sure the "Allow guests to log into this computer" is not checked.
	
	Alternatively, run the following commands:
	
	`sudo dscl . -create /Users/Guest AuthenticationAuthority ";basic;"`
	`sudo dscl . -create /Users/Guest passwd "*"`
	`sudo dscl . -create /Users/Guest UserShell "/sbin/nologin"`

Audit	Run the following command
	
	`dscl . -read /Users/Guest AuthenticationAuthority`
	
	The result should be:
	
	`AuthenticationAuthority: ;basic;`

Additional Info	By default, the guest account is enabled for access to sharing services, but is not allowed to log in to the computer. The guest account does not need a password when it is enabled to log in to the computer.

1.4.2.8 *Disable "Allow guests to connect to shared folders"*

Explanation	If files need to be shared, a dedicated file server should be used. If file sharing on the client Mac must be used, then only authenticated access should be used. Guest access allows guest to access files they might not need access to.
Context	System
Level	1
Scoring Status	Scorable
Caveats	None

Remediation	In System Preferences: Account, click on the Guest user.
	Make sure the "Allow guests to connect to shared folders" is not checked.
	
	Alternatively, run the following commands:
	
	For AFP sharing:
	<pre>sudo defaults write /Library/Preferences/com.apple.AppleFileServer \
	guestAccess -bool no</pre>
	for SMB sharing:
	<pre>sudo defaults write \
	/Library/Preferences/SystemConfiguration/com.apple.smb.server \
	AllowGuestAccess -bool no</pre>

Audit	In System Preferences: Account, click on the Guest user.
	Make sure the "Allow guests to connect to shared folders" is not checked.
	
	Alternatively, run the following command:
	
	For AFP sharing:
	<pre>defaults read /Library/Preferences/com.apple.AppleFileServer
	guestAccess</pre>
	for SMB sharing:
	<pre>defaults write \
	/Library/Preferences/SystemConfiguration/com.apple.smb.server \
	AllowGuestAccess</pre>
	Make sure the results are `0`.

Additional Info	This setting is not enabled by default in Snow Leopard, but the sharing services themselves are all turned off. The guest account does not need a password for access to shared services when it is enabled.

1.4.3 Bluetooth Preferences Action Items

Bluetooth can be a very useful technology, but it can also leave an unprotected computer open to compromise. Bluetooth is best used in a secure environment where unauthorized users have no physical access near the Mac. If Bluetooth is used, it should be secured properly (see below). Also, please note a recommendation earlier in this document to completely disable Bluetooth.

1.4.3.1 Disable Bluetooth by using System Preferences for each user account

Explanation	As stated earlier, Bluetooth can be very useful, but can also expose a Mac to certain risks. Unless specifically needed and configured properly, Bluetooth should be turned off
Context	User
Level	1
Scoring Status	Scorable
Caveats	Removes Bluetooth functionality. See recommendations in sections 2.4.3.3 and 2.4.3.4 on how to secure Bluetooth if it is used.

Remediation	In System Preferences: Bluetooth, uncheck the "On" box.
	
	Alternatively, run the following commands:
	
	`sudo defaults write /Library/Preferences/com.apple.Bluetooth \`
	`ControllerPowerState -int 0`
	
	`sudo killall -HUP blued`

Audit	In System Preferences: Bluetooth, verify "On" box is unchecked. Alternatively, run the following command: defaults read /Library/Preferences/com.apple.Bluetooth ControllerPowerState and make sure the value returned is 0.
Additional Info	None

1.4.3.2 Disable Bluetooth internet connection sharing

Explanation	Bluetooth internet sharing can expose a Mac and the network to certain risks and should be turned off.
Context	System
Level	1
Scoring Status	Scorable
Caveats	None

Remediation	In System Preferences: Bluetooth, Advanced options, turn off "Share my internet connection with other Bluetooth devices"
	
	Alternatively, run the following commands:
	
	`sudo defaults write /Library/Preferences/com.apple.Bluetooth \`
	`PANServices -int 0`
	
	`sudo killall -HUP blued`

Audit	In System Preferences: Bluetooth, Advanced options, verify "Share my internet connection with other Bluetooth devices" if off
	Alternatively, run the following commands
	`defaults read /Library/Preferences/com.apple.Bluetooth PANServices`
	and make sure the value returned is `0`.
Additional Info	This setting is turned off by default in Snow Leopard.

1.4.3.3   If Bluetooth is used, turn off "Discoverable" when not needed

Explanation	When Bluetooth is set to "discoverable" mode, the Mac sends a signal indicating that it's available to "pair" with another Bluetooth device. When in discoverable state an attacker could gain access to data on the Mac. Use discoverable mode when "pairing" a Bluetooth device to the Mac, but once the "pairing" is complete, turn discoverable mode off.
Context	User
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	In System Preferences: Bluetooth, turn Discoverable off when not actively "pairing" a Bluetooth device.
Audit	None
Additional Info	None

1.4.3.4   Show Bluetooth status in menu bar

Explanation	By showing the Bluetooth status in the menu bar, a small Bluetooth icon is placed in the menu bar. This icon quickly shows the status of Bluetooth, and can allow the user to quickly turn Bluetooth on or off.
Context	User
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	In System Preferences: Bluetooth, turn Show Bluetooth Status In Menu Bar on.
Audit	None
Additional Info	None

1.4.4 CDs & DVDs Preferences Actions Items

Explanation	Managing automatic actions, while useful in very few situations, is unlikely to increase security on the computer and does complicate the users experience and add additional complexity to the configuration. These settings are user controlled and can be changed without Administrator privileges unless controlled through MCX settings or Parental Controls. Unlike Windows Auto-run the optical media is accessed through Operating System applications, those same applications can open and access the media directly. If optical media is not allowed in the environment the optical media drive should be disabled in hardware and

	software
Context	User
Level	2
Scoring Status	Not Scorable
Caveats	None
Remediation	
Audit	
Additional Info	None

1.4.5 Date & Time Preferences Action Items

As stated earlier in this document, setting the correct date and time can be very important. Use the Set date & time automatically feature.

1.4.5.1   Enter correct time settings

Explanation	Having the correct date, time, time zone, and daylight saving time setting (if applicable) on a Mac is very important. File creation and modification dates use the system time. Log entries use the system time. Kerberos may not operate correctly if the time on the Mac is off by more than 5 minutes, which can affect Apple's single sign-on feature, Active Directory logons, and other features.
Context	System
Level	1
Scoring Status	Scorable
Caveats	If port 123 (the NTP port) is blocked by a firewall, the automatic date and time feature will not work. If the port is blocked, a time server accessible behind the firewall must be used to set the date and time automatically. A mix of internal and external time servers is recommended for mobile systems.
Remediation	In System Preferences: Date & Time, Select the Time Zone tab. Make sure the correct Time Zone is selected. Next, select the Date & Time tab. Make sure the "Set date & time automatically" checkbox is checked. If your organization runs its own time server, enter its address in the field. You can enter multiple time servers by separating them with a space, listing them in order of preference. Alternatively, perform the following: Using `sudo`, edit `/private/etc/hostconfig` and change the `TIMESYNC` entry to -YES- Using `sudo`, edit `/private/etc/ntp.conf` and enter desired servers. For example: ``` server time.mycompany.com preferred server time.apple.com ``` Then restart the time daemon: ``` sudo launchctl load -w \ /System/Library/LaunchDaemons/org.ntp.ntpd.plist ```
Audit	In System Preferences: Date & Time select the Date & Time tab. Make sure the "Set date & time automatically" checkbox is checked.

	Alternatively, run the following commands:
	
	`cat /etc/hostconfig | grep TIMESYNC`
	
	Make sure the results are:
	`TIMESYNC=-YES-`
	
	`cat /etc/ntp.conf`
	
	Make sure the results list desired time servers. For example:
	
	`server time.apple.com`
	
	Verify the `/System/Library/LaunchDaemons/org.ntp.ntpd.plist` job is running
	
	`cat /System/Library/LaunchDaemons/org.ntp.ntpd.plist | grep Disabled`
	
	make sure the results are blank.

Additional Info	`man ntp.conf` http://support.ntp.org/bin/view/Main/WebHome By default, a system set up with the Mac OS X Setup Assistant will use one of Apple's time servers. Be sure you understand the ramifications if you do not use fully-qualified domain names (FQDN) or IP addresses when specifying your time servers.

1.4.5.2   Use an internal Software Update mechanism

Explanation	Apple offers a Software Update Service in the Mac OS X Server product. If your organization uses such a service, set the computer to use your internal server. Other products are available as well to manage patching and enable consistent configuration management. Consistent patching and management adds greatly to the security of computers inside an organization.
Context	System
Level	2
Scoring Status	Scorable
Caveats	Your computer will not be able to get updates using Software Update unless it has network access to the organizational software update server.

Remediation	The Software Update Service setting can be set though a managed Mac environment using Apple's Workgroup Manager.
	
	Alternatively, the following command can be run from Terminal:
	
	`sudo defaults write /Library/Preferences/com.apple.SoftwareUpdate \`
	`CatalogURL <url>`
	
	where `<url>` is the URL to the update server.
	
	Use the following command to clear the setting and use the Apple, Inc., software

	update server: ``` sudo defaults delete /Library/Preferences/com.apple.SoftwareUpdate \ CatalogURL ```
Audit	Run the following comment to determine if a software update server is defined. ``` defaults read /Library/Preferences/com.apple.SoftwareUpdate CatalogURL ``` Note: in a Mac OS X server environment the software update server may be defined using MCX and may be located in a different place.
Additional Info	Mac OS X defaults to using Apple's Software Update servers.

1.4.5.3 Maintain a software asset inventory external to the computer

Explanation	With the introduction of Mac OS X 10.6.6, Apple added a new application, App Store, which resides in the Applications directory. This application allows a user with admin privileges and an Apple ID to browse Apple's online App Store, purchase (including no cost purchases) and install new applications, bypassing corporate software inventory controls. Any admin user can install software in the /Applications directory whether from internet downloads, thumb drives, optical media, cloud storage or even binaries through email. Even standard users can run executables if permitted. The source of the software is not nearly as important as a consistent audit of all installed software patch compliance and appropriateness.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	A single user desktop whether the user, administrator and the person approving software are all the same person probably does not need to audit software inventory to this extent. It is helpful in the case of stability problems or malware however
Remediation	Export Apple System Profiler information through the built-in or other third party tools on an organizationally defined timetable
Audit	Scan systems on a monthly basis and determine the number of unauthorized pieces of software that are installed. Verify that if an unauthorized piece of software is found one month, it is removed from the system the next.
Additional Info	https://www.sans.org/critical-security-controls/control.php?id=2

1.4.6 Desktop & Screen Saver Preferences Action Items

1.4.6.1 Set a short inactivity interval for the screen saver

Explanation	By obscuring the screen with a picture, graphic, or just an opaque color, the screen saver can keep prying eyes off of an unattended screen and potentially sensitive information.
Context	User
Level	1
Scoring Status	Scorable

Caveats	None
Remediation	In System Preferences: Desktop & Screen Saver, Screen Saver Tab, make sure the Start screen saver slider is to a reasonably low value. Alternatively, run the following command: `defaults -currentHost write com.apple.screensaver idleTime -int 900` where 900 is the number of idle seconds until the screen saver starts. A logout of the user may be required for the new settings to take effect.
Audit	Open System Preferences: Desktop & Screen Saver, Screen Saver Tab, make sure the Start screen saver slider is to a reasonably low value (like 15 minutes). Alternatively, run the following command: `defaults -currentHost read com.apple.screensaver idleTime` and verify the setting is adequately low (`<= 900`)
Additional Info	None

1.4.6.2 *Disable users or admins to login to another users active and locked session*

Explanation	Administrators with rights to manage the device do not necessarily have rights to access everything the user of the computer has rights to including email, web applications and mounted shares and disk images and there are definitely privacy and personal information implications by allowing everyone with administrative rights access to any users active session
Context	User
Level	1
Scoring Status	Scorable
Caveats	While Fast user switching is a workaround for some lab environments especially where there is even less of an expectation of privacy this setting change may impact some maintenance workflows

Remediation	Edit `/etc/authorization` `system.login.screensaver` setting to the following:
	
	`<key>system.login.screensaver</key>`
	`            <dict>`
	`                    <key>class</key>`
	`                    <string>rule</string>`
	`                    <key>comment</key>`
	`                    <string>The owner can unlock the`
	`screensaver.</string>`
	`                    <key>rule</key>`
	`                    <string>authenticate-session-owner</string>`

Audit	`grep -ir "<string>authenticate-session-owner-or-admin</string>" /etc/authorization` No results will be returned if the system is configured as recommended.
Additional Info	None

1.4.7 Energy Saver Preferences Action Items

1.4.7.1   Disable sleeping the computer when connected to power

Explanation	In some institutions certain software must be run that requires the computer to be awake. In these situations the computer should not be set to sleep.
Context	System
Level	2
Scoring Status	Scorable
Caveats	Not allowing the computer to sleep will use more power and increase the cost to operate the computer. This must be weighed against the needs of the organization.
Remediation	In System Preferences: Energy Saver, drag the slider for "Put the computer to sleep..." to never. Alternatively, use the following command: `sudo pmset -c sleep 0`
Audit	In System Preferences: Energy Saver, verify the slider for "Put the computer to sleep..." to never. Alternatively, use the following command: `pmset -g	grep sleep`  and verify the value returned is `0`
Additional Info	`man pmset`

1.4.7.2   Verify Display Sleep is set to a value larger than the Screen Saver

Explanation	If the Screen Saver is used to lock the screen, verify the Display Sleep settings are longer than the Screen Saver setting. If the display goes to sleep before the screen saver activates, the computer will appear to be off, but will be unprotected.
Context	System
Level	1
Scoring Status	Scorable
Caveats	None
Remediation	In System Preferences: Energy Saver, drag the slider for "Put the display(s) to sleep..." to a reasonable number, but longer than the screen saver setting. The Mac will display a warning if the number is too short. Alternatively, use the following command: `sudo pmset -c displaysleep 0` Note: The `-c` flag means "wall power." Different settings must be used for other power sources.
Audit	In System Preferences: Energy Saver, verify the slider for "Put the display(s) to sleep..." to a reasonable number, but longer than the screen saver setting. The Mac will display a warning if the number is too short.

	Alternatively, use the following command:
	`pmset -g | grep displaysleep`
	and verify the value returned is longer than the Screen Saver, if the Screen Saver is used to lock the screen.
Additional Info	`man pmset`

1.4.7.3 Disable "Wake when the modem detects a ring" for all power settings

Explanation	Unless the computer is used to receive facsimiles or is used as a modem access point for incoming calls, this feature is not needed. An attacker could remotely wake a machine using a modem, then attack the machine through the internet.
Context	System
Level	1
Scoring Status	Scorable
Caveats	None.
Remediation	In System Preferences: Energy Saver, Options tab, make sure the "Wake when the modem detects a ring" is not checked. Alternatively, use the following command: `sudo pmset -c ring 0` Note: The `-c` flag means "wall power." Different settings must be used for other power sources.
Audit	In System Preferences: Energy Saver, Options tab, verify the "Wake when the modem detects a ring" is not checked. Alternatively, use the following command: `pmset -g | grep ring` and verify the value returned is `0`.
Additional Info	`man pmset`

1.4.7.4 Disable "Wake for Ethernet network administrator access" for power adapter settings

Explanation	This option might be used in certain organizations. The feature, sometimes called the "Wake-on-LAN", is only useful for those organizations that specifically need it. Otherwise it should be turned off so an attacker cannot use it to wake your computer remotely.
Context	System
Level	1
Scoring Status	Scorable
Caveats	Management programs like Apple Remote Desktop Administrator use this feature to wake computers. If turned off, such management programs will not be able to wake a computer over the LAN. If the wake-on-LAN feature is needed, do

	not turn off this feature.
Remediation	In System Preferences: Energy Saver, Options tab, make sure the "Wake for Ethernet network administrator access" is not checked. Alternatively, use the following command: `sudo pmset -c womp 0` Note: The `-c` flag means "wall power." Different settings must be used for other power sources.
Audit	In System Preferences: Energy Saver, Options tab, verify the "Wake for Ethernet network administrator access" is not checked. Alternatively, use the following command: `pmset -g | grep womp` and verify the value returned is `0`.
Additional Info	`man pmset`

1.4.8 Exposé & Spaces Preferences Action Items

Management of the Exposé and Spaces preferences are useful primarily to change "hot corner" settings that affect the screen saver and display sleep.

1.4.8.1 Do not set any screen corner to Disable Screen Saver

Explanation	The screen saver should be set to turn on after a period of inactivity, and should require a password to dismiss. Disabling the screen saver would disable the screen lock.
Context	User
Level	2
Scoring Status	Scorable
Caveats	None

Remediation	In System Preferences: Exposé & Spaces, make sure none of the Active Screen Corners are set to disable the screen saver.
	
	The screen corners can be set using the defaults command, but the permutations of combinations are many. The plist file to check is `~/Library/Preferences/com.apple.dock` and the keys are:
	
	`wvous-bl-corner`
	`wvous-br-corner`
	`wvous-tl-corner`
	`wvous-tr-corner`
	
	There are also modifier keys to check and various values for each of these keys. A value of `6` for any of corners should not be allowed (`6` = disable screen saver). If any value is `6`, change the value to `1` (which means no action). Also change the corresponding wvous-xx-modifier key to `1048576`

Audit	In System Preferences: Exposé & Spaces, make sure none of the Active Screen Corners are set to disable the screen saver.

	Alternatively, Use the following command when logged is as each user: ```read ~/Library/Preferences/com.apple.dock``` verify none of the *-corner keys has a value of "`1`".
Additional Info	None

1.4.8.2   Set a screen corner to Start Screen Saver

Explanation	A user should be able to activate the screen saver quickly.
Context	User
Level	1
Scoring Status	Scorable
Caveats	None

Remediation	In System Preferences: Exposé & Spaces, make sure at least one Active Screen Corner is set to Start Screen Saver. Make sure the user knows about this feature.
	
	The screen corners can be set using the defaults command, but the permutations of combinations are many. The plist file to check is ```~/Library/Preferences/com.apple.dock``` and the keys are
	
	```wvous-bl-corner```
	```wvous-br-corner```
	```wvous-tl-corner```
	```wvous-tr-corner```
	
	There are also modifier keys to check and various values for each of these keys. A value of `5` means the corner will start the screen saver. The corresponding wvous-xx-modifier key should be set to `0`.

Audit	In System Preferences: Exposé & Spaces, make sure at least one Active Screen Corner is set to Start Screen Saver. Make sure the user knows about this feature. Alternatively, Use the following command: ```read ~/Library/Preferences/com.apple.dock``` verify at least one of the *-corner keys has a value of `5`.
Additional Info	None

1.4.8.3   Do not set any screen corner to Sleep Display

Explanation	When this feature is used the screen goes blank but moving the mouse or pressing a button brings up the screen again with no password required. The screen saver (with its lock) will still kick in after X minutes, but the user could be lulled into a false sense of security if she sees her screen is blank and the screen saver has not activated.
Context	User
Level	1
Scoring Status	Scorable
Caveats	None

Remediation	In System Preferences: Exposé & Spaces, make sure none of the Active Screen Corners are set to Sleep Display. The screen corners can be set using the defaults command, but the permutations of combinations are many. The plist file to check is `~/Library/Preferences/com.apple.dock` and the keys are ``` wvous-bl-corner wvous-br-corner wvous-tl-corner wvous-tr-corner ``` There are also modifier keys to check and various values for each of these keys. A value of `10` for any of corners should not be allowed (`10` = sleep display). If any value is `10`, change the value to `1` (which means no action). Also change the corresponding wvous-xx-modifier key to `1048576`.
Audit	In System Preferences: Exposé & Spaces, make sure none of the Active Screen Corners are set to Sleep Display. Alternatively, Use the following command: ``` read ~/Library/Preferences/com.apple.dock ``` verify none of the *-corner keys has a value of `10`.
Additional Info	None

1.4.9 Keyboard & Mouse Action Items

1.4.9.1 Disable "Allow Bluetooth devices to wake this computer"

Explanation	Unless you are using a Bluetooth keyboard or mouse in a secure environment, there is no reason to allow Bluetooth devices to wake the computer. An attacker could use a Bluetooth device to wake a computer and then attempt to gain access.
Context	User
Level	1
Scoring Status	Scorable
Caveats	This setting is only available in the Mac is equipped with Bluetooth.
Remediation	In System Preferences: Keyboard & Mouse, Bluetooth tab, make sure the "Allow Bluetooth devices to wake this computer" is not checked. Alternatively, run the following command: ``` defaults -currentHost write \ ~/Library/Preferences/com.apple.Bluetooth \ BluetoothSystemWakeEnable -bool 0 ```
Audit	In System Preferences: Keyboard & Mouse, Bluetooth tab, make sure the "Allow Bluetooth devices to wake this computer" is not checked. Alternatively, run the following command: ``` defaults -currentHost read \ ~/Library/Preferences/com.apple.Bluetooth BluetoothSystemWakeEnable ```

	And verify the result is `0`.
Additional Info	None

1.4.10 Network Preferences Action Items

Configuring the network from the CLI is extremely tricky, but some options can be configured using the networksetup command

1.4.10.1 Create network specific locations

Explanation	The network location feature of the Mac is very powerful tool to mange network security. By creating different network locations, a user can easily (and without administrative privileges) change the network settings on the Mac. By only using the network interfaces needed at any specific time, exposure to attackers is limited.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	A little understanding of how the Network System Preferences pane works is required.
Remediation	Create multiple network locations as needed. Delete the Automatic location for any device that does not use multiple network services set for DHCP or dynamic addressing. If network services like FireWire, VPN, AirPort or Ethernet are not used by a specific device class those services should be deleted: 1. Select Edit Locations from the Locations popup menu. 2. Select the Automatic location. 3. Click the minus button for any unneeded service. Create network locations as needed. Ideally, if your goal is to limit which interfaces can be used at any given time, one network location for each interface should be created. See the Appendix C for an example.
Audit	Open System Preferences: Network Verify each network location is set up properly.
Additional Info	Deleting the Automatic location cannot be undone.

1.4.10.2 Disable AirPort

Explanation	If Airport is installed and not needed, disable it. There is no need to allow attackers a possible route to the Mac.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	In System Preferences: Network, select the Airport interface and click the minus button or turn the Airport card off.
Audit	In System Preferences: Network, select the Airport interface and verify the Airport card off.

Additional Info	None

1.4.10.3 Enable Show AirPort Status in Menu Bar

Explanation	If an Airport or other wireless card is installed, show the AirPort status in the menu bar so that user can quickly determine if AirPort is on or off. If on, the user can quickly turn it off if AirPort interface should be off.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	In System Preferences: Network, select the Airport interface, then click the Advanced button. Turn on Show AirPort status in menu bar.
Audit	In System Preferences: Network, select the Airport interface, then click the Advanced button. Verify Show AirPort status in menu bar is on.
Additional Info	AirPort is Apple's marketing name for its 802.11b, g, and n wireless interfaces.

1.4.10.4 Disable Bluetooth

Explanation	If Bluetooth is installed and not needed, disable it. There is no need to allow attackers a possible route to the Mac.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	In System Preferences: Network, select the Bluetooth interface and click the minus button or turn Bluetooth off.
Audit	In System Preferences: Network, select the Bluetooth interface and verify that Bluetooth is not offered as a network interface option.
Additional Info	None

1.4.10.5 Disable IPv6

Explanation	Unless used, IPv6 should be turned off for each interface. IPv6 is not widely used yet, so most people can turn this off until needed.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	None
Remediation	In System Preferences: Network, select the each active interface then click the Advanced button. Find the Configure IPv6 popup menu and set it to Off.
Audit	In System Preferences: Network, select the each active interface then click the Advanced button. Find the Configure IPv6 popup menu and verify it is Off.
Additional Info	None

1.4.11 Print & Fax Preferences Action Items

1.4.11.1 Only use known printers

Explanation	The Mac's ability to browse and find printers is very good. One should only print to a known printer. When at a public location, such as a hotel or trade show, many printers may appear available in the Print & Fax panel. Only print to a known printer.
Context	User
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	This rule cannot be implemented technically. One just has to use one's judgment when printing.
Audit	None
Additional Info	None

1.4.11.2 Disable receiving faxes

Explanation	Unless fax reception is required, the option should be turned off. While there is no known vector to attack a Mac using a fax, an attacker could attempt to use fax reception to determine if a modem is connected to a computer.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	This option is only available if the Mac is equipped with a fax modem.
Remediation	In System Preferences: Print & Fax, Fax tab, turn off fax reception.
Audit	In System Preferences: Print & Fax, Fax tab, verify fax reception is off. This option will only be present if the computer is equipped with a fax modem.
Additional Info	None

1.4.12 QuickTime Preferences Action Items

One of the few known common attack vectors is QuickTime. Securing QuickTime can help protect your computer against malware.

1.4.12.1 Do not install third-party QuickTime software

Explanation	Do not install any QuickTime software unless the source is known and trusted.
Context	System and User
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	Check that software in `/Library/QuickTime` and `~/Library/QuickTime` is valid.
Audit	Check that software in `/Library/QuickTime` and `~/Library/QuickTime` is valid.
Additional Info	None

1.4.12.2 Disable "Play Movies automatically"

Explanation	QuickTime is used in browsers to play audio and video content. When the browser sees such content the browser passes off control to QuickTime through

	its Web browser plug-in. QuickTime can be set to start playing this content immediately. Some content may contain malicious code embedded in the audio or video. Ensure the user wants to play the embedded content by turning off the "Play Movie Automatically" option.
Context	User
Level	1
Scoring Status	Not Scorable
Caveats	The user will need to press a play button to play the content in the browser.
Remediation	In System Preferences: QuickTime: Browser tab, disable "Play movies automatically"
Audit	In System Preferences: QuickTime: Browser tab, verify "Play movies automatically" is disabled.
Additional Info	None

1.4.13 Security Preferences Action Items

1.4.13.1 Require a password to wake the computer from sleep or screen saver

Explanation	Sometimes referred to as a "screen lock" this option will keep the casual user away from your Mac when the screen saver has started.
Context	User
Level	1
Scoring Status	Scorable
Caveats	None
Remediation	In System Preferences: Security, General tab, check "Require a password to wake the computer from sleep or screen saver" Alternatively, run the following command. The current user will need to log off and on for changes to take effect. ``` defaults -currentHost write \ com.apple.screensaver askForPassword -int 1 ```
Audit	In System Preferences: Security, General tab, verify "Require a password to wake the computer from sleep or screen saver" is on Alternatively, run the following command: ``` defaults -currentHost read com.apple.screensaver askForPassword ``` and verify the setting is 1
Additional Info	This only protects the system when the screen saver is running.

1.4.13.2 Disable automatic login

Explanation	Having a computer automatically log in bypasses a major security feature (the login password) and can allow a casual user access to sensitive data.
Context	System
Level	1
Scoring Status	Not Scorable

Caveats	None
Remediation	In System Preferences: Security, General tab, check "Disable Automatic Login". Note: Automatic login can also be disabled in System Preferences: Accounts.
Audit	In System Preferences: Security, General tab, verify "Disable Automatic Login" is checked.
Additional Info	None

1.4.13.3 Require a password to unlock each System Preferences pane

Explanation	By requiring a password to unlock System Preferences, a casual user is less likely to compromise the security of the Mac.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	In System Preferences: Security, General tab, check "Require a password to unlock each System Preferences pane." Alternatively, using `sudo`, edit the `/private/etc/authorization` file. This file should be backed up first and then edited. This is a critical file for OS X operations and should edited with the greatest of care. 1. Find `<key>system.preferences</key>` 2. Then find `<key>shared</key>` 3. Then replace `true` with `false`.
Audit	In System Preferences: Security, General tab, verify "Require a password to unlock each System Preferences pane" is checked.
Additional Info	None

1.4.13.4 Automatically update safe downloads list

Explanation	Files downloaded via applications such as Safari, iChat, and Mail are checked for safety at the time that they are opened. If a file is identified as containing known malware, the system will display a dialog that alerts you to move it to the Trash. You should empty the Trash to finalize the removal of the file. Apple maintains a list of known malicious software that is used during the safe download check to determine if a file contains malicious software, the list is updated daily by a background process.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	Apple will push updates to the computer for malware definition files
Remediation	In System Preferences: Security, General tab, ensure that "Automatically update safe downloads list" is checked
Audit	
Additional Info	https://support.apple.com/kb/HT4651

1.4.13.5 Disable "automatic logout" after a period of inactivity

Explanation	If the machine automatically logs out, unsaved work might be lost. The same level of security is available by using a Screen Saver and the "Require a password to wake the computer from sleep or screen saver" option.
Context	System
Level	1
Scoring Status	Scorable
Caveats	This option might be appropriate for kiosk Macs or for other organizational reasons.

Remediation	In System Preferences: Security, General tab, uncheck "Log out after X minutes of inactivity."
	
	Alternatively, run the following command
	
	`sudo defaults write /Library/Preferences/.GlobalPreferences \`
	`com.apple.autologout.AutoLogOutDelay -int 0`

Audit	In System Preferences: Security, General tab, verify "Log out after X minutes of inactivity" is unchecked.
	
	Alternatively, run the following command
	
	`defaults read /Library/Preferences/.GlobalPreferences \`
	`com.apple.autologout.AutoLogOutDelay`
	
	and verify the result is `0`.

Additional Info	None

1.4.13.6 Use secure virtual memory

Explanation	Passwords and other sensitive information can be extracted from insecure virtual memory, so it's a good idea to secure virtual memory. If an attacker gained control of the Mac, the attacker would be able to extract user names and passwords or other kinds of data from the virtual memory swap files.
Context	System
Level	1
Scoring Status	Scorable
Caveats	Use the secure virtual memory will tax the computer a little bit as it has to encrypt and decrypt virtual memory. The small overhead, however, is worth the added security. Note: Encrypting virtual memory is not foolproof. Proof of concept attacks by security researchers have recently shown that computer memory, even in a Mac, is readable for up to ten minutes after shut down! When shutting down a Mac, make sure the computer is protected from physical access for at least ten minutes.
Remediation	In System Preferences: Security, General tab, check "Use secure virtual memory." Alternatively, run the following command

| | ```
sudo defaults write /Library/Preferences/com.apple.virtualMemory \
UseEncryptedSwap -bool yes
```<br><br>A reboot is required to make a change. |
| Audit | In System Preferences: Security, General tab, verify "Use secure virtual memory" is checked.<br><br>Alternatively, run the following command<br><br>```
defaults read /Library/Preferences/com.apple.virtualMemory \
UseEncryptedSwap
```<br><br>verify the result is 1 |
| Additional Info | Enabling secure virtual memory in Snow Leopard also encrypts the hibernation file if the safe sleep feature is enabled on compatible hardware. |

1.4.13.7 Disable remote control infrared receiver

Explanation	It's very humorous to watch a jokester use an Apple remote at a Mac trade show. Macs all over the place start to obey the remote and the unsuspecting user is left bewildered. More importantly, a remote could be used to page through a document or presentation, thus revealing sensitive information. The solution is to turn off the remote and only turn it on when needed. Optionally, the user can "pair" the remote with the computer. Pairing will force the computer to only respond to commands from the paired remote. Pairing a remote is discussed in section 2.4.13.7.
Context	System
Level	1
Scoring Status	Scorable
Caveats	Requires the user to turn on the remote when needed. An administrative password is needed to activate the remote.
| Remediation | In System Preferences: Security, General tab, check "Disable remote control infrared receiver".<br><br>Alternatively to disable the remote use the following command:<br><br>```
sudo defaults write \
/Library/Preferences/com.apple.driver.AppleIRController \
DeviceEnabled -bool no
``` |
| Audit | In System Preferences: Security, General tab, verify that "Disable remote control infrared receiver" is checked or the computer is paired with a specific remote.<br><br>Alternatively, run the following command:<br><br>```
defaults read /Library/Preferences/com.apple.driver.AppleIRController
```<br><br>Verify the DeviceEnabled is 0 or the UIDFilter does not equal none |

Additional Info	None

1.4.13.8 Pair the remote control infrared receiver

Explanation	If a remote is used often with a computer, the remote can be "pair" to work with the computer. This will allow on the paired remote to work on that computer.
Context	System
Level	1
Scoring Status	Scorable
Caveats	None
Remediation	See http://docs.info.apple.com/article.html?artnum=302545 for complete instructions.
Audit	Open System Preferences: Security and verify the remote is paired. Alternatively, run the following command: `defaults read /Library/Preferences/com.apple.driver.AppleIRController` Verify the `UIDFilter` does not equal `none`.
Additional Info	Pairing your Apple Remote with your computer: http://docs.info.apple.com/article.html?artnum=302545

1.4.13.9 Enable FileVault for every account

Explanation	FileVault offers protection for data at rest. This means that the data is only protected when the user is not logged in, which is useful if the computer is stolen.
Context	User
Level	2
Scoring Status	Not Scorable
Caveats	There are many caveats to using FileVault. Apple does not provide a means for organizational key recovery if the password is lost. Double the size of the user's home directory is required to be available on the hard drive when FileVault for the user is turned on. Not everything on the disk is encrypted, so a false sense of security may ensue when using FileVault. And finally, FileVault can cause a significant slowdown of the system. All that said, however, FileVault is still a good method to provide data at rest protection. There are also challenges in using FileVault with Directory accounts, particularly around external password changes and password expiration on off-line computers. **Note:** Encrypting user data is not foolproof. Proof of concept attacks by security researchers have recently shown that computer memory, even in a Mac, is readable for up to ten minutes after shut down! When shutting down a Mac, make sure the computer is protected from physical access for at least ten minutes.
Remediation	In System Preferences: Security, FileVault tab, press the "Set Master Password" button and set a master password. Set and secure this master password according to your organization's policies.

	Press the Turn FileVault on button to turn FileVault on. Apple offers a workaround solution for organizations to maintain a common Master password. Contact your Apple representative for more information.
Audit	In System Preferences: Security, FileVault tab, verify FileVault is on for each user.
Additional Info	http://www.apple.com/sg/macosx/features/filevault/

1.4.13.10 Enable firewall protection

Explanation	Apple's firewall will protect your computer from certain incoming attacks. Apple offers three firewall options: Allow all, Allow only essential, and Allow access for specific incoming connections. Unless you have a specific need to allow incoming connection (for services such as SSH, file sharing, or web services), set the firewall to "Allow only essential services," otherwise use the "Allow access for specific incoming connections" option. Only enable stealth mode if approved by your network engineering, scanning or security team.
Context	System
Level	1
Scoring Status	Scorable
Caveats	None
| Remediation | In System Preferences: Security, Firewall tab, select "Allow only essential services" or "Set access for specific services and applications".<br><br>Alternatively, run the following command:<br><br>```
sudo defaults write \
/Library/Preferences/com.apple.alf globalstate -int <value>
```<br><br>where `<value>` is:<br><br>• `0` = off<br>• `1` = on for specific services<br>• `2` = on for essential services |
| Audit | In System Preferences: Security, Firewall tab, verify "Allow only essential services" or "Set access for specific services and applications" is selected.<br><br>Alternatively, run the following command:<br><br>```
defaults read /Library/Preferences/com.apple.alf globalstate
```<br><br>verify the value returned is `1` or `2` |
| Additional Info | http://docs.info.apple.com/article.html?artnum=306938 |

1.4.13.11 Enable Secure Keyboard Entry in terminal.app

Explanation	In a multi-user environment it is possible for keystrokes to be intercepted. If an admin is typing sensitive commands in `terminal.app` it is suggested that secure keyboard entry is enabled.

Context	User
Level	2
Scoring Status	Scorable
Caveats	None
Remediation	From `terminal.app` click on Terminal and then click on "Secure Keyboard Entry"
Audit	Launch `terminal.app` and make sure "Secure Keyboard Entry" is checked.
Additional Info	http://docs.info.apple.com/article.html?path=Terminal/2.1/en/5386.html

1.4.14 Sharing Preferences Action Items

1.4.14.1 Change the computer name

Explanation	If the computer is used in an organization that assigns host names, it is a good idea to change the computer name to the host name. This is more of a best practice than a security measure. If the host name and the computer name are the same, computer support may be able to track problems down easier.
Context	System
Level	2
Scoring Status	Scorable
Caveats	Of minimal security benefit
Remediation	In System Preferences: Sharing, change the computer name to the host name. Alternatively, use the following command: `sudo systemsetup -setcomputername <host name>`
Audit	In System Preferences: Sharing, verify the computer name is set to the host name. Alternatively, use the following command: `systemsetup -getcomputername`
Additional Info	None

1.4.14.2 Configure Screen Sharing

Explanation	Screen Sharing uses the open source VNC protocol to let one computer observe or control the screen on another computer. Apple Screen Sharing is encrypted (using a proprietary encryption protocol), so others cannot eavesdrop on a screen sharing session. The most important aspect of securing screen sharing is to make sure only the correct people can observe or control the Mac. Apple allows for a few options when configuring screen sharing and each has its place for a secure Mac. These option are not mutually exclusive. 1. Screen Sharing off This is the most secure option. 2. Anyone may request permission to control screen This is the second most secure option. When a remote user attempts to share the screen, the Mac will prompt the local user for permission. If the local user doesn't grant permission, the remote user cannot share the screen. If a local

	user is not at the Mac to grant permission, then the screen cannot be shared. 3. VNC viewers may control screen with password This is the least secure option since the remote user only needs to know the password. 4. Allow access to all users of the Mac, or specific users (or groups of users) Allowing access to only users with accounts on the Mac, or if a directory service (like Open Directory or Active Directory) is used, specific users or groups, allows some restriction of who can share the screen. Any authorized user would be able to observe or control the screen without the express permission of the local user. This option should only be used when necessary (possibly in a school environment).
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	A thorough understanding of each setting's advantages and disadvantages is necessary when turning Screen Sharing on.
Remediation	In System Preferences: Sharing, turn on Screen Sharing only if necessary. Configure Screen Sharing according to personal or organizational needs, but be aware of the implications of each option.
Audit	None
Additional Info	None

1.4.14.3 Disable File Sharing

Explanation	Apple's File Sharing uses a combination of many technologies: FTP, SMB (Windows sharing) and AFP (Mac sharing). Generally speaking, file sharing should be turned off and a dedicated, well-managed file server should be used to share files. If file sharing must be turned on, the user should be aware of the security implications of each option. Turning on File Sharing automatically shares the entire hard drive to anyone with an account on the Mac, or anyone who can access the Mac using a network account. File and folder access control restrictions are enforced by default, so user Mary cannot access user Joe's Documents folder (by default). Specific access controls can be relaxed or strengthened for specific folders in the Sharing System Preference pane. Each method of sharing files has advantages and disadvantages. Regardless of which method used, the folder and file access permissions must be controlled to make sure only the correct data is shared. The three ways to share files using File Sharing are:[1] 1. Apple File Protocol (AFP) AFP under Snow Leopard automatically uses encrypted logins, so this method

---

[1] Technically the Mac can share files other ways out of the box: Secure Copy Protocol (scp), secure File Transfer Protocol (sftp), and Network File System (NFS). scp and sftp are a subset of the Remote Login feature and are discussed is the Remote Login section of this document. Apple doesn't provide a GUI means of enabling NFS, so the NFS protocol will not be discussed in this document. NFS poses significant security risks and should only be configured by an experienced system administrator familiar with inherent NFS risks.

of sharing files is fairly secure. The entire hard disk is shared to administrator user accounts. Individual home folders are shared to their respective user accounts. Users' "Public" folders (and the "Drop Box" folder inside) are shared to any user account that has sharing access to the computer (i.e. anyone in the "staff" group, including the guest account if it is enabled).

2. File Transfer Protocol (FTP)
   FTP send password via clear text and thus is very insecure. FTP is commonly used for anonymous upload and download of files where security is of less concern. FTP should not be used on a client Mac except in rare case for temporary anonymous sharing.

3. Server Message Block (SMB), Common Internet File System (CIFS)
   When Windows (or possibly Linux) computers need to access file shared on a Mac, SMB/CIFS file sharing is commonly used. Apple warns that SMB sharing stores passwords is a less secure fashion than AFP sharing and anyone with system access can gain access to the password for that account. When sharing with SMB, each user that will access the Mac must have SMB enabled.

Context	System
Level	1
Scoring Status	Scorable
Caveats	A thorough understanding of each protocol's advantages and disadvantages, as well as an understanding of what folders and files are shared is necessary when turning File Sharing on.

Remediation	In System Preferences: Sharing, turn on Screen Sharing only if necessary. Configure Screen Sharing according to personal or organizational needs, but be aware of the implications of each option.
	
	To turn off AFP from the command line:
	
	`sudo launctl unload -w \`
	`/System/Library/LaunchDaemons/com.apple.AppleFileServer.plist`
	
	To turn off FTP from the command line:
	
	`sudo launctl  unload -w /System/Library/LaunchDaemons/ftp.plist`
	
	To turn off SMB sharing from the CLI:
	
	`sudo defaults delete \`
	`/Library/Preferences/SystemConfiguration/com.apple.smb.server \`
	`EnabledServices`
	
	`sudo launctl unload -w /System/Library/LaunchDaemons/nmbd.plist`
	`sudo launctl unload -w /System/Library/LaunchDaemons/smbd.plist`

Audit	In System Preferences; Sharing, File Sharing; Options, verify only the needed sharing services are on. Alternatively, run the following commands: `launchctl list`

	and look for the various services listed above in the remediation section.
Additional Info	If authenticated ftp is used all console and SSH users should be entered into the `/etc/ftpusers` list to deny ftp access for those users with full access.

1.4.14.4 Secure SMB

Explanation	SMB can be configured using the `/etc/smb.conf` file. By default, SMB is fairly secure, but it can be made more secure with a few additions to the `/etc/smb.conf` file.
Context	System
Level	2
Scoring Status	Scorable
Caveats	May provide more restrictions on SMB sharing than needed.

Remediation	Using `sudo`, edit the file `/etc/smb.conf`
	Find the `[Global]` section and add the following lines:
	
	`; don't allow any anonymous connections`
	`restrict anonymous = 2`
	
	`; do not allow guest access (this is the default)`
	`guest OK = no`
	
	`; only allow NTLMv2 and LMv2 response`
	`client ntlmv2 auth = yes`

Audit	`cat /etc/smb.conf` and look for the options as listed in the remediation section.
Additional Info	`man smb.conf`

1.4.14.5 Turn off Printer Sharing

Explanation	Printer Sharing makes the Mac into a print server. Attackers could attempt to exploit the print server to gain access to the Mac. As with File Sharing, Printer Sharing is best left off and a dedicated, well-managed print server or a printer with built-in IP network capability is recommended.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	In System Preferences: Sharing, turn off Printer Sharing.
Audit	In System Preferences: Sharing, verify Printer Sharing is off for each printer listed.
Additional Info	None

1.4.14.6 Disable Web Sharing

Explanation	Web Sharing uses the Apache 2.2.x Web server to turn the Mac into an HTTP/Web server. When Web Sharing is on, files in `/Library/WebServer/Documents` as well as each user's "Sites" folder are made available on the Web. As with File Sharing, Web Sharing is best left off and a dedicated, well-managed Web server is recommended.
Context	System

Level	1
Scoring Status	Scorable
Caveats	None

Remediation	In System Preferences: Sharing, turn on Web Sharing only if necessary.
	
	To turn off Web sharing from the command line:
	
	`sudo launchctl  unload -w \`
	`/System/Library/LaunchDaemons/org.apache.httpd.plist`

Audit	In System Preferences: Sharing, verify Web Sharing is off. Alternatively, run the following command: `launchctl list` and look for a line with "`apache`."
Additional Info	Snow Leopard includes Apache 2.2.

1.4.14.7 Secure Web Sharing

Explanation	Web Sharing can be configured using the `/etc/apache2/httpd.conf` file (for global configurations). By default, Apache is fairly secure, but it can be made more secure with a few additions to the `/etc/apache2/httpd.conf` file.
Context	System
Level	2
Scoring Status	Scorable
Caveats	The `UserDir` directive below will stop the "Sites" folders from being shared on the Web. Only the `/Library/WebServer/Documents` folder is shared if `UserDir` is off. A user might not understand the relevance of the "Sites" folder and may place sensitive files in the "Sites" folder that would be shared if Web Sharing is turned on. Also, an attacker might attempt to determine user names using Web requests if `UserDir` is on. Do not disable `UserDir` if your needs dictate that the "Sites" folders for users need to be shared.

Remediation	Using `sudo`, edit the`/apache2/httpd.conf` file and add the following to the bottom of the file. Restart Web Sharing after making the changes (turn it off and on again)
	
	`# limit the information the server gives out about its version`
	`ServerTokens Prod`
	
	`# limit the information the server gives out about its version`
	`ServerSignature Off`
	
	`# turns off all username-to-directory translations except those`
	`# explicitly named with the enabled keyword this directive`
	`# turns off the Sites folder for every user as a Web share`
	`# Only the DocumentRoot folder is shared`
	`UserDir Disabled`
	
	`# causes the core server and mod_proxy to return`
	`# a 405 (Method not allowed) error to the client.`

| | ```
TraceEnable Off
``` |
| Audit | `cat /etc/apache2/httpd.conf` and look for the remediation above. |
| Additional Info | http://httpd.apache.org/docs/2.2/ |

1.4.14.8 Secure Remote Login

Explanation	Remote Login is Apple's implementation of Secure Shell (SSH). SSH is an effective and efficient method for remote management of devices. If the service is not configured appropriately enabling remote login can open major security holes. Do not enable SSH if not needed. The configuration file for SSHD should be configured such that if the service is enabled it is appropriately hardened.
Context	System
Level	2
Scoring Status	Scorable
Caveats	Organizational and personal requirements will dictate which should be used.
| Remediation | Set the following in `sshd_config`:<br><br>```
GSSAPIAuthentication=yes
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes

X11Forwarding no
Protocol 2
PermitRootLogin no
MaxAuthTries 4          # or less
IgnoreRhosts yes
HostbasedAuthentication no
PermitEmptyPasswords no
PermitUserEnvironment no
ClientAliveInterval 300 # or less
ClientAliveCountMax 0
AllowUsers <userlist>   # or AllowGroups
LogLevel VERBOSE
LoginGraceTime 120      # or less
```<br><br>Note: A prior recommendation sets the Banner directive for Remote Login |
| Audit | See Remediation |
| Additional Info | `man sshd_config` |

1.4.14.9 Configure Remote Management

Explanation	Remote Management is the client portion of Apple Remote Desktop (ARD) < http://www.apple.com/remotedesktop/>. Remote Management has a screen sharing component similar to the Screen Sharing feature described above. Remote Management can also be used by administrators to install software, report on, and generally manage client Macs. ARD is mostly likely to be used in an organization and not by home users. The screen sharing options in Remote Management are identical to those in the

Screen Sharing section. In fact, only one of the two can be configured. If Remote Management is used, refer to the Screen Sharing section above on issues regard screen sharing.

Other features of Remote Management should be configured if the service is used. One option is to "Show Remote Management status in the menu bar." Turning this option on allows the user to see if screen sharing or other remote management features are being used.

More security settings of relevance are found after clicking on the Options button. Only those options needed by the Remote Management Administrator should be turned on.

The final security concern with Remote Management is the list of users that access the Mac with Remote Management. The easiest and least secure method, is to have the same username and password for a Remote Management administrator on every Mac in an organization. If this one name/password combination is compromised, the entire network of Macs is compromised.

The second method would be to have a different username/password combination on each Mac. This is difficult to implement since one would need to remember a large number of passwords and usernames, or one would need to write them down, thus creating a target for compromise.

The ideal solution is to use a directory service (like Open Directory or Active Directory) and only allow group access. This method allows an organization to add or remove people to the directory group as needed, thus controlling access to the network of Macs. There are four groups used by ARD for this purpose: `ard_admin`, `ard_interact`, `ard_manage` and `ard_reports`. Therefore, combining or nesting local or network groups and user accounts may meet your needs. Various versions of Mac OS X and ARD may or may not allow the use of these groups, particularly if groups are nested within groups.

Context	System
Level	1
Scoring Status	Not Scorable
Caveats	A wide variety of configuration permutations are possible with Remote Management. Remote Management should be configured by an experienced administrator.
Remediation	In System Preferences: Sharing, turn on Remote Management if necessary. If turned on, configure the screen sharing options as discussed above in the Screen Sharing section. Turn on the option: "Show Remote Management status in the menu bar"

Only turn on the options in the Options button if necessary.

Use a directory service to allow Remote Management access. Do not use a common username/password across multiple Macs. |
| Audit | Use the `kickstart` program to set or determine Remote Management settings. |
| Additional Info | `/System/Library/CoreServices/RemoteManagement/ARDAgent.app/Contents/Resources/kickstart -help` |

1.4.14.10 Disable Remote Apple Events

Explanation	Apple Events is a technology that allows one program to communicate with other programs. Remote Apple Events allows a program on one computer to communicate with a program on a different computer. Typically Remote Apple Events is used to automate a business process. Unless needed, Remote Apple Events should be turned off. If needed, it should be configured with the least access granted as possible. If Mac OS 9 is not being used, the option to allow events from OS 9 should be turned off. If OS 9 events are needed, a username and password should be used.
Context	System
Level	1
Scoring Status	Scorable
Caveats	None
Remediation	In System Preferences: Sharing, turn on Remote Apple Events only if necessary. If turned on, add users to the Allow Access for list if possible To turn off Remote Apple Events from the command line: `sudo launchctl  unload -w /System/Library/LaunchDaemons/eppc.plist`
Audit	In System Preferences: Sharing, verify Remote Apple Events is off. Alternatively, run the following command: `launchctl list	grep -I eppc` There should be no results.
Additional Info	None

1.4.14.11 Disable Xgrid Sharing

Explanation	Xgrid is Apple's distributed computing technology. Xgrid should be turned off unless specifically needed. If needed, access should be controlled using the Single Sign On option.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	In System Preferences: Sharing, turn on XGrid only if necessary. If turned on, select Single Sign On for the Authentication method.
Audit	None
Additional Info	http://www.apple.com/server/macosx/technology/xgrid.html The single sign on option for Xgrid uses Kerberos.

1.4.14.12 Disable Internet Sharing

Explanation	Internet Sharing uses the open source `natd` process to share an internet connection with other computers and devices on a local network. Unless specifically required, Internet Sharing should be turned off. If used, it should only

	be turned on when actual sharing is needed. A much better solution is a dedicated router (available for as little as $10US). Apple makes a number of certified compatible routers.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	In System Preferences: Sharing, turn on Internet Sharing only if necessary. Alternatively, run the following commands: ``` sudo defaults write \ /Library/Preferences/SystemConfiguration/com.apple.nat \ NAT -dict Enabled -int 0 sudo launchctl unload -w \ /System/Library/LaunchDaemons/ com.apple.InternetSharing.plist ```
Audit	In System Preferences: Sharing, verify Internet Sharing is off. Alternatively, run the following commands:
Additional Info	http://www.apple.com/wifi/

1.4.14.13 Completely disable sharing services

Explanation	Various sharing services can offer an attacker a conduit to compromise a system. Unless absolutely needed, sharing should be turned off or completely disabled so that it cannot be turned on. If any of these services are needed, a better solution is a dedicated server.
Context	System
Level	2
Scoring Status	Scorable
Caveats	The recommended way to disable these services can be reversed by an administrative user or possibly by a system update. Removal of the `LaunchDaemons` does not prevent an attacker with elevated privileges from re-creating them, copying them from another Snow Leopard-based computer, or running the sharing executables outright.
Remediation	The following files should be moved or deleted from `/System/Library/LaunchDaemons/`: • `com.apple.AppleFileServer.plist` (AFP) • `ftp.plist` (FTP) • `smbd.plist` (SMB) • `org.apache.httpd.plist` (Web) • `eppc.plist` (Remote Apple Events) • `com.apple.mDNSResponder.plist` (Bonjour) • `com.apple.mDNSResponderHelper.plist` (Bonjour) • `com.apple.xgridagentd.plist` (Xgrid)

	• `com.apple.xgridcontrollerd.plist` (Xgrid) • `com.apple.InternetSharing.plist` (Internet Sharing)
Audit	Verify the files are removed for the service(s) disabled.
Additional Info	

1.4.15 Software Update Preferences Action Items

Note: Software Update preferences must be set for each user.

1.4.15.1 Disable "Check for updates" for standard users

Explanation	Since most updates require an administrative password to install, there is little need to notify standard users when updates are available. The exception would be if the standard user also has an administrator account on the same Mac.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	Only disable for standard users that do not have an administrator account.
Remediation	In System Preferences: Software Update, turn on "Check for updates" for administrator accounts, and for standard users that also have an administrator account. Turn off "Check for updates" for all others.
Audit	None
Additional Info	None

1.4.15.2 Download important updates automatically

Explanation	Generally, it is not a good idea to have a computer automatically download operating level software patches from unknown sites automatically. Since the Software Update process will either use the Apple's own Software Update service or one provided by the organization (via Mac OS X Server), there is little benefit in turning this option off.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	The security benefits are minimal.
Remediation	In System Preferences: Software Update, turn off "Download important updates automatically".
Audit	None
Additional Info	This option only downloads, but does not install, the updates.

1.4.15.3 Transfer installer packages from a test-bed computer

Explanation	In the software update program, one can choose to download only or install and keep packages. Ideally one would download the updates from Apple, install them on a test computer, then test the functionality and compatibility of the new software. If approved, the installer packages would be moved to production machines for installation.
Context	System
Level	2
Scoring Status	Not Scorable

Caveats	This process is probably too burdensome for the SoHo market but is recommended for high sensitivity environments.
Remediation	In Apple Menu: Software Update, select File Download Only when updates are available. Update packages are stored in the user's `~/Download` folder. Test updates for compatibility and functionality and if approved, deploy the updates to other Macs.
Audit	None
Additional Info	Downloading and vetting packages for various kinds of Apple hardware may be difficult to manage even for an organization. Some updates apply only to specific computer models. The Software Update utility, in contrast, only makes updates available if they apply to the current computer — but it lists all updates that apply.

1.4.16 Sound Preferences Action Items

1.4.16.1 Change sound input device to Line In

Explanation	Apple provides no way to turn off the internal microphone (if so equipped). A remote attacker could enable the microphone and listen in on potentially sensitive conversations. The only way to limit the microphone is to turn the input volume off and to set the input to line in. Even if done, however, the internal microphone can still be turned on by a remote hacker or by an application running on the Mac. The safest method to disable the internal microphone it to have it disconnected by an authorized Apple technician.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	The microphone can easily be turned on by an application or remote attacker.
Remediation	If the Mac is equipped with an internal microphone, in System Preferences: Sound, Input tab, set the input to Line In.
Audit	If the Mac is equipped with an internal microphone, in System Preferences: Sound, Input tab, verify the input is set to Line In.
Additional Info	None

1.4.16.2 Minimize input volume for all inputs

Explanation	Apple provides no way to turn off the internal microphone (if so equipped). A remote attacker could enable the microphone and listen in on potentially sensitive conversations. The only way to limit the microphone is to turn the input volume off and to set the input to line in. Even if done, however, the internal microphone can still be turned on by a remote hacker or by an application running on the Mac. The safest method to disable the internal microphone it to have it disconnected by an authorized Apple technician.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	The microphone can easily be turned on by an application or remote attacker.
Remediation	If the Mac is equipped with an internal microphone, in System Preferences: Sound, Input tab, set the input volume all the way to left (off). Click on each input device and set the volume to off for each device.

Audit	If the Mac is equipped with an internal microphone, in System Preferences: Sound, Input tab, verify the input volume is set all the way to left (off). Click on each input device and verify the volume is set to off for each device.
Additional Info	None

1.4.17 Speech Preferences Action Items

Note: Speech preferences must be set for each user.

1.4.17.1 Only enable speech recognition in a secure environment

Explanation	Apple's speech recognition allows a user to speak a finite list of commands that are recognizable by the computer. If configured improperly, anyone within earshot of the Mac can initiate these actions. Use of speech recognition should be in a secure environment where only the user of the Mac can issue commands.
Context	User
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	In System Preferences, Speech, Speech Recognition tab, turn off Speakable Items unless in a secure environment.
Audit	In System Preferences, Speech, Speech Recognition tab, verify Speakable Items is off.
Additional Info	Apple's speech recognition is listener independent, does not require training, and is optimized for a speaker within about 21 inches of the built-in microphones on Macintosh models. It may work better with a speech-quality microphone. A brief calibration routine for each user (and often, in each new aural environment) is recommended. The speech command sets enabled by default include: • Address Book • Global Speakable Items (such as "What time is it" and "What day is it") • Application Specific Items (provided in the bundles of running applications) • Application Switching. Additional Speakable Items are found in `~/Library/Speech/Speakable Items`, a directory which does not exist by default (and is not in the User Template).

1.4.17.2 Configure Speech Recognition to use a Listening Key

Explanation	Speech Recognition can be configured to listen continuously or only when a specific key is pressed. Listening continuously can allow anyone within earshot of the Mac to initiate an operation on the Mac. Configure speech recognition to use a Listening Key to commands are only executed when the Mac user desires them to be.
Context	User
Level	1
Scoring Status	Not Scorable
Caveats	None

Remediation	In System Preferences, Speech, Speech Recognition tab, select "Listen only while key is pressed".
Audit	In System Preferences, Speech, Speech Recognition tab, verify "Listen only while key is pressed" is selected.
Additional Info	None

1.4.17.3   Use headphones if you enable text to speech, or turn text to speech off

Explanation	When using the Text to Speech feature, use headphones to others cannot hear what the computer is saying. The computer may convert sensitive text to speech, so limit who can hear it.
Context	User
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	In System Preferences, Speech, Text to Speech tab, turn off all options or wear headphones.
Audit	None
Additional Info	None

1.4.18 Spotlight Preferences Action Items

1.4.18.1   Prevent Spotlight from searching all confidential folders

Explanation	Spotlight is Apple's search technology built into the operating system. By default it indexes every file on any local hard drive. While spotlight will enforce access control restrictions to limit access to files, the index itself may contain information about sensitive files that others should not see. The Spotlight System Preference Pane allows the user to exclude volume, folders, and data types from being indexed.
Context	User and System
Level	1
Scoring Status	Not Scorable
Caveats	Adding folders or volumes to the privacy settings will restrict searching for information in those folders and volumes. For example, adding ~/Library/Mail will disable the ability to search through the body of Mail messages, even within the Mail application. Also, authentication is not required to add or remove items to the exclusion list. Any user can remove items from the exclusion list.
Remediation	In System Preferences: Spotlight, Search Results tab turn off any categories that should not be indexed. In System Preferences: Spotlight, Privacy tab add any volumes or folders that contain sensitive data. Alternatively you can disable spotlight from indexing and search specific volumes with the following command: `sudo mdutil -E -i off <volumename>`

Audit	None
Additional Info	None

1.4.18.2 Prevent Spotlight from searching backup folders or volumes

Explanation	Spotlight is Apple's search technology built into the operating system. By default it indexes every file on any local hard drive. If a local hard drive is used for backup, spotlight will find the original and the backup of a file. The user may edit the backup file and lose changes if the back up file overwrites the backup with the original.
Context	User and System
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	In System Preferences: Spotlight, Privacy tab add any volumes or folders that contain backups.
Audit	In System Preferences: Spotlight, Privacy tab verify all backup volumes or folders are in the privacy list.
Additional Info	None

1.5 Data Maintenance and Encryption Action Items

1.5.1 Backup

Explanation	Backing up is very important. This point cannot be stressed enough. Apple includes Time Machine to make backing up easier. Numerous third party free and commercial products are also available to back up one's Mac. A good backup scheme can mitigate the loss of data if a Mac is compromised, lost, stolen, or becomes unusable.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	None
Remediation	When using Time Machine, simply connect and external drive to the Mac and the Mac will ask if you want to use the drive as a backup drive. Select yes.

When using other software, follow the software's instructions to backup. |
| Audit | None |
| Additional Info | None |

1.5.2 Secure Home Folders

Explanation	By default the Mac is set up to allow every user to see into the top level of the home folder of other users. This allows user to drop files into the "Drop Box" folders of other users. This also allows users to see newly-created files and folders in the top level of other users' home folders but not within the standard subfolders such as "Documents" and "Library." This access to the top of other users' home folders may not be desirable. To resolve this potential revelation of sensitive information, permissions should be set on home folder to restrict

	access to the owner of the folder.
Context	User
Level	2
Scoring Status	Scorable
Caveats	If implemented, users will not be able to use the "Public" folders in other users' home folders. "Public" folders with appropriate permissions would need to be set up in the /Shared folder.
Remediation	Open Terminal and enter: sudo chmod 700 /Users/<username> where <username> is the name of each user. This command has to be run for each user account with a local home folder.
Audit	Run the following command: `ls -l /Users/` verify that each user home folder looks like `drwx------`
Additional Info	None

1.5.3 Encrypt sensitive files

Explanation	Sensitive files should be encrypted, especially when sent over e-mail, the network, or on removable media or laptops. FileVault will encrypt all files in the home directory, including Mail, but only at rest (when the user is logged out). In order to encrypt files when in transit (mailed, copied over the network, on removable media), encryption software is required. Apple provides encrypted disk images as a feature of Disk Utility, and Apple Mail supports encryption for Mail. There are also numerous third party products that provide for individual or enterprise level encryption and key management. Which product to use and how to use it is beyond the scope of this document.
Context	User
Level	2
Scoring Status	Not Scorable
Caveats	Encryption is complicated and very commonly site and user specific.
Remediation	Encrypt sensitive data whenever possible.
Audit	None
Additional Info	None

1.5.4 Securely erase files in the Finder

Explanation	When a file is put into the trash and trash is emptied, only the directory entry for the file is deleted; the data in the file is not actually deleted. Think of a magic book library. When the librarian wants to remove a book she just removes the card catalog card for the book. The book stays on the shelf until the space is needed. When space is needed, pages from the book are removed until the needed space is made available. Until all the space of the original book is needed, some pages may remain on the shelf. The computer operates in a similar fashion. The data from the file is still on the

	hard drive until the operating systems needs the space. "Undelete" software is available to recover these files, and special disk reading software is available to look at partial remains of the file if part of its space is used. To be sure a deleted file is actually deleted, the Mac has a feature called Secure Empty Trash (under the Finder menu). When selected the Mac not only removes the file information from the file directory, the Mac also overwrites the data in the file with meaningless data, thus preventing the file from being recovered. Use Secure Erase Trash to erase sensitive files. Finder: Preferences: Advanced allows the user to set Empty Trash Securely as the default. The command line tool `srm` is also available as an alternative to `rm`.
Context	User
Level	1
Scoring Status	Not Scorable
Caveats	Secure Empty Trash can take a long time. If the user's home folder is using FileVault that extra time is being taken to erase part of an encrypted file.
Remediation	When emptying the trash, use Finder: Secure Empty Trash if sensitive files are in the trash. If sensitive files are commonly deleted, set the Finder: Preferences: Advanced Empty Trash Securely option to on. Use the `srm` command in Terminal when deleting sensitive files from the CLI.
Audit	None
Additional Info	`man srm`

1.5.5 Securely erase partitions

Explanation	Using the erase capability of Disk Utility (found on the Mac OS X Install DVD) will only erase the directory structure of disk and leave its contents intact. To make sure everything on the partition is erased, the Secure Erase feature of the Disk Utility must be used. Unless an organizational hard drive disposal policy must be followed, a 7 pass wipe secure erase should be used before a hard drive is discarded, sold, or transferred to another party. If time permits, a 35 pass wipe can be used, but a 7 pass wipe is generally adequate.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	This process can take a long time, possibly days if the 35 pass wipe is used on a high-capacity disk. Perform this on a laptop only if it is connected to power with its power adapter.

Remediation	1. Open /Applications/Disk Utility.
	2. Select the partition to erase on in the left panel.
	3. Select the Erase tab.
	4. Click on the Security Option button.
	5. Choose "Zero out data", then OK. Use a 7 or 35 pass erase if required.
	6. Click the erase button
Audit	None
Additional Info	According to Apple the "7-Pass Erase" option conforms to the DoD 5220.22-M specification. This specification calls for three passes, but Disk Utility performs seven. See https://support.apple.com/kb/HT3680

1.5.6 Securely erase free space

Explanation	If sensitive files have been erased without using Secure Erase, Mac OS X offers an additional way to securely erase all of the free space on a drive. This action will make it even harder for anyone to recover deleted files from the Mac.
Context	System
Level	2
Scoring Status	Not Scorable
Caveats	Can take a very long time (hours). If interrupted, the free space may not be easily recoverable.
Remediation	1. Open /Applications/Disk Utility
	2. Select the desired partition on in the left panel
	3. Select the Erase tab
	4. Click the Erase Free Space... button
	5. Choose the desired option
	6. Click the Erase Free Space button.
	Warning: if performing this operation on a laptop, make sure the power adaptor is plugged in. Also, even though there is a cancel option, we do not recommend canceling.
	The following CLI command will securely erase free space:
	`sudo diskutil secureErase freespace [1|2|3] /`
	where `[1|2|3]` is one of the following:
	• 1 = single pass erase
	• 2 = 7 pass erase
	• 3 = 35 pass erase
Audit	None
Additional Info	`man diskutil`

1.5.7 Repair disk permissions after installing software or software updates

Explanation	Sometimes file permissions get set differently from the desired permissions. A

	number of reasons might cause this, and most are beyond the control of the user. Every time a package is installed, the package leaves a receipt that tells the computer what files were installed and what their permissions on disk should be. Using the repair permissions feature of Disk Utility, the permissions of most program files can be reset to the desired values.
Context	System
Level	1
Scoring Status	Not Scorable
Caveats	If custom permissions were set on items in /Applications or /Library, these permissions may need to be reset.
Remediation	1. Open Applications: Disk Utility. 2. Select the startup disk in the left panel. 3. Select the First Aid tab. 4. Click on the Repair Permission button Alternatively the command can be run from Terminal: `diskutil repairPermissions /` Permissions can be repaired when started up from a Mac OS X Install DVD, but Apple recommends running it from a fully-updated Mac OS X system instead.
Audit	None
Additional Info	Apple recommends running repair permissions from an up-to-date system disk, rather than the system installer DVD. http://docs.info.apple.com/article.html?artnum=25751 If the system is not maintained by a configuration management tool that manages permissions, a good best practice is to schedule a permission repair to occur at least monthly. Tools like `launchd` can be used (use `Lingon` as a GUI front end for `launchd`). Also, the command line above can be placed in the file `/etc/monthly.local` and the command will be executed monthly (`/etc/weekly.local` will execute the command weekly).

1.6 Network Services Configuration Action Items

1.6.1 Secure Bonjour

Explanation	Bonjour is an auto-discovery mechanism for TCP/IP devices. Because Bonjour can enumerate devices and services within a local subnet it can simplify device discovery from an internal rogue or compromised host. An attacker could use Bonjour's multicast DNS feature to discover a vulnerable or poorly-configured service or additional information to aid a targeted attack. The actual discovery is performed via DNS Service Discovery (DNS-SD). DNS on Mac OS X (10.6) is integrated with Bonjour and should not be turned off. If required the Bonjour advertising service can be disabled
Context	System
Level	2

Scoring Status	Not Scorable
Caveats	Anything Bonjour discovers is already available on the network and probably discoverable with network scanning tools. The security benefit of disabling Bonjour for that reason is minimal. Also note that some applications, like Final Cut Studio and AirPort Base Station management, may not operate properly if the `mDNSResponder` is turned off. Early OS X releases provided extensive information when scanned on the local subnet, 10.6 does not disclose as much information and changing the configuration should align with the likelihood of an internal scan and the asset information that would be disclosed

Remediation	To disable Bonjour advertising service without disabling Bonjour queries and DNS.:
	
	 1. Make a back up copy of the `mDNSResponder.plist` file as a precaution.
	 2. Open the `mDNSResponder.plist` file in Terminal using your preferred text editor. Below is a sample command:
	
	 ```sudo nano \ "/System/Library/LaunchDaemons/com.apple.mDNSResponder.plist"```
	
	 3. Add `<string>-NoMulticastAdvertisements</string>` to the array in the `ProgramArguments` section. For example:
	
	 The following:
	
	 ```<key>ProgramArguments</key> <array> <string>/usr/sbin/mDNSResponder</string> <string>-launchd</string> </array>```
	
	 becomes:
	
	 ```<key>ProgramArguments</key> <array> <string>/usr/sbin/mDNSResponder</string> <string>-launchd</string> <string>-NoMulticastAdvertisements</string> </array>```
	
	 4. Save the file.

Additional Info	https://support.apple.com/kb/HT3789?viewlocale=en_US

1.6.2 Use an outbound network detection system

Explanation	The Apple firewall will prevent unwanted incoming network traffic, but will not prevent unwanted outbound network traffic. Unwanted outbound traffic might include spyware or malware traffic. Included with Mac OS X is a firewall called `ipfw`, which is what Apple used as the main firewall in prior releases of the operating system. Apple doesn't use `ipfw` anymore, but still includes it in Snow Leopard. Configuring `ipfw` to prevent unwanted outbound traffic is beyond the scope of this document. Various third party software products, notably Little Snitch, have outbound traffic firewall capabilities.

Context	System
Level	2
Scoring Status	Not Scorable
Caveats	Firewalls are complex and the rules can be difficult to set up.
Remediation	Use a firewall product that blocks unwanted outbound traffic.
Audit	None
Additional Info	http://seaotter.berkeley.edu/cab/mac-firewalls/ has a good run down of firewall products for Mac OS X

1.7 System Integrity Validation Action Items

1.7.1 Increase the retention time for system.log and secure.log

Explanation	Many log files are archived and retained for 5 days based on the default Mac OS X configuration. Snow Leopard includes a new utility (`newsyslog`) to configure how log files are stored and retained. Two important logs should be retained for longer than the default 5 days: syslog.log and secure.log.
Context	System
Level	2
Scoring Status	Scorable
Caveats	None
Remediation	Backup then, using `sudo`, edit `/etc/newsyslog.conf` Change the 5 in the count column to 30 for the syslog.log line and the secure.log line.
Audit	`cat /etc/newsyslog.conf` and verify the count is 30 for system.log and secure.log
Additional Info	`man newsyslog.conf` Snow Leopard includes the Apple System Log (ASL) facility, which is a replacement for syslog but provides compatibility with it. See `man syslogd` and `man asl.conf` for more information.

1.8 Application Security

1.8.1 Safari should not open safe files after downloading

Explanation	Safari will automatically run or execute what it considers safe files. This can include installers and other files that execute on the operating system. Malware has taken advantage of this setting through drive-by attacks.
Context	Safari
Level	1
Scoring Status	Not Scorable
Caveats	User will have to manually open files from the downloads folder
Remediation	1. Start the Safari program. 2. Select **Preferences** from the Safari menu on the left side of the menu bar. 3. Choose the "General" tab. 4. Uncheck the box that says "Open 'safe' files after downloading". Quit Safari.
Audit	
Additional Info	

2 Appendix A: Change History

Date	Version	Changes for this version
November 23rd, 2011	1.0.0	Public Release